



*Files are in Adobe format.
Download the newest version from Adobe.*

2010 Homeland Security Symposium & Exhibition

"America's Homeland Leaders Talk Risk"

Arlington, VA

28 - 29 September 2010

Agenda

Tuesday, 28 September 2010

Keynote Address

- Ms. Caryn Wagner, Under Secretary for Intelligence & Analysis (I&A), U.S. Department of Homeland Security

Panel: *International Terrorism – The Threat from Abroad*

- Mr. Robert Cruz, Vice President, Terrorism & Global Response, Hiscox International Insurance

Panel: *Domestic Terrorism – The Threat at Home*

- Mr. Brian H. Dodd, Assistant Special Agent in Charge, Special Operations Division, Drug Enforcement Administration, U.S. Department of Justice
- Mr. Akmal Ali, J.D., Office of SAFETY Act Implementation, Science and Technology Directorate, U.S. Department of Homeland Security

Panel: *The Wrath and Consequences of "Mother Nature"*

- Ms. Laura K. Furgione, Deputy Assistant Administrator for Weather Services, National Oceanic and Atmospheric Administration (NOAA); Deputy Director, National Weather Service (NWS)
- Lieutenant Rex Strickland, Operations Chief, Fairfax County Urban Search and Rescue
- Mr. Charley Shimanski, Senior Vice President of Disaster Services, American Red Cross
- Mr. Christopher Royse, Senior Program Director for Global Threat Reduction and Security Initiatives, Parsons Infrastructure & Technology

Panel: *Border Security*

- Mr. Michael J. Fisher, Chief, U.S. Border Patrol, U.S. Department of Homeland Security
- Vice Admiral David Pekoske, USCG (Ret), Executive Vice President, A-T Solutions, Inc.; former Vice Commandant, U.S. Coast Guard

Wednesday, 29 September 2010

Government Keynote Address

- Mr. Andy Purdy, Chief Cybersecurity Strategist, Computer Sciences Corporation; former Acting Director, National Cyber Security Division/US-CERT, U.S. Department of Homeland Security

Panel: *Cyber Threats and Enhancing Security of the IT Infrastructure*

- Mr. Paul Beckman, CISSP, Chief Information Security Officer (CISO), Information Technology Security Office Risk Management Division, HQ, Office of the Chief Information Officer (CIO), U.S. Department of Homeland Security
- Mr. Scott Charbo, Vice President, Accenture; former Chief Information Officer, U.S. Department of Homeland Security
- Mr. David Wiley, Chief Technology Officer, L-3 Corporation, STRATIS

Panel: *Critical Infrastructure Protection and Resilience*

- Ms. Yazmin Seda-Sanabria, Senior Program Manager, Critical Infrastructure Protection & Resilience (CIPR) Program Office of Homeland Security, HQ, U.S. Army Corps of Engineers

2010 HOMELAND SECURITY SYMPOSIUM & EXHIBITION

“America’s Homeland Leaders Talk Risk”



SHERATON NATIONAL HOTEL, ARLINGTON, VA

SEPTEMBER 28-29, 2010

WWW.NDIA.ORG/MEETINGS/0490

EVENT #0490

AGENDA

LOCATION

Sheraton National Hotel
900 South Orme Street
Arlington, VA 22204
(703) 521-1900

REGISTRATION

Assembly Foyer

GENERAL SESSION

Commonwealth South

EXHIBIT AREA

Commonwealth North, Cavalier

ATTIRE

Appropriate dress for the symposium is business coat & tie for civilians and Class A uniform or uniform of the day for military personnel.

ID BADGES

During symposium registration and check-in, each attendee will be issued an identification badge. Please be prepared to present a valid picture ID. Badges must be worn at all symposium functions.

2010 HOMELAND SECURITY SYMPOSIUM & EXHIBITION

September 28-29, 2010
Sheraton National Hotel, Arlington, VA

"America's Homeland Leaders Talk Risk"

MONDAY, SEPTEMBER 27, 2010

12:00 PM – 5:00 PM **Registration Open & Exhibitor Move-in**
Assembly Foyer

TUESDAY, SEPTEMBER 28, 2010

7:00 AM – 6:30 PM **Registration**
Assembly Foyer

7:00 AM – 8:00 AM **Continental Breakfast**
South Lobby

8:00 AM – 8:15 AM **Welcome & Opening Remarks**
Commonwealth South

Major General Barry D. Bates, USA (Ret), Vice President, Operations, NDIA

Mr. Rich Cooper, Principal, Catalyst Partners, LLC;
Chairman, NDIA Homeland Security Division

8:15 AM – 9:00 AM **Keynote Address**
Commonwealth South

Ms. Caryn Wagner, Under Secretary for Intelligence & Analysis (I&A), U.S. Department of Homeland Security

9:00 AM – 6:30 PM **Exhibit Area Open**
Commonwealth North, Cavalier

9:00 AM – 10:30 AM **Panel: International Terrorism – The Threat from Abroad**
Commonwealth South

There is no country immune from the threat of terrorism. A threat once thought only limited to the Middle East, terrorism remains the weapon of choice of extremists around the globe. Combating it requires the cross-border coordination of intelligence, law enforcement officials and emergency resources to mitigate against it. Assembled experts will share emerging trends and what is being done to reduce against these threats.

Moderator: Mr. Rich Cooper, Principal, Catalyst Partners, LLC; Chairman, NDIA Homeland Security Division

- Mr. Robert Cruz, Vice President, Terrorism & Global Response, Hiscox International Insurance
- Ms. Tina Gabbrielli, Director, Office of Risk Management and Analysis, U.S. Department of Homeland Security
- Mr. John P. Woods, Deputy Assistant Director, National Security, Homeland Security Investigations, Immigration & Customs Enforcement (ICE), U.S. Department of Homeland Security
- Mr. Ben Tucker, Senior Vice President, Property Specialized Risk Group, Marsh, Inc.

10:30 AM – 11:00 AM Networking Break in Exhibit Area
Commonwealth North, Cavalier

11:00 AM – 12:15 PM Panel: Domestic Terrorism – The Threat at Home
Commonwealth South

From violent attacks on government office buildings and national landmarks to the emergence of more extremist groups, terrorism is now home on American soil. To adapt to these conditions, public and private sector officials and public safety officers have had to implement new training, technology and coordination to address these threats. Assembled experts will talk about their lessons learned and how they are adapting.

Moderator: Mr. Bill Carroll, Senior Vice President, Strategic Planning, SiloSmashers

- Mr. Brian H. Dodd, Assistant Special Agent in Charge, Special Operations Division, Drug Enforcement Administration, U.S. Department of Justice
- Mr. John P. Woods, Deputy Assistant Director, National Security, Homeland Security Investigations, Immigration & Customs Enforcement (ICE), U.S. Department of Homeland Security
- Mr. Akmal Ali, J.D., Office of SAFETY Act Implementation, Science and Technology Directorate, U.S. Department of Homeland Security

12:15 PM – 1:30 PM Networking Lunch in Exhibit Area
Commonwealth North, Cavalier

1:30 PM – 5:00 PM View Exhibits Only

1:30 PM – 3:00 PM Panel: The Wrath and Consequences of “Mother Nature”
Commonwealth South

Recent hurricanes, earthquakes and floods have shown how Mother Nature and her extremes can be devastating to individuals, properties and critical infrastructures. It is critically important to know what types of disasters strike in the areas where you live, travel or do business so that you and your organization can be prepared. From tornadoes to floods, snow storms and heat waves, different threats and conditions require different precautions before, during and after weather-related/natural emergencies. Assembled experts will give a first hand report of how they have addressed these specific threats to mitigate risk and enhance overall preparedness.

Moderator: The Honorable Nancy Harvey Steorts, former Chairman, U.S. Consumer Product Safety Commission; President, Nancy Harvey Steorts & Associates

- Ms. Laura K. Furgione, Deputy Assistant Administrator for Weather Services, National Oceanic and Atmospheric Administration (NOAA); Deputy Director, National Weather Service (NWS)
- Lieutenant Rex Strickland, Operations Chief, Fairfax County Urban Search and Rescue
- Mr. Charley Shimanski, Senior Vice President of Disaster Services, American Red Cross
- Mr. Christopher Royse, Senior Program Director for Global Threat Reduction and Security Initiatives, Parsons Infrastructure & Technology

PROCEEDINGS

Proceedings will be available on the web through the Defense Technical Information Center (DTIC) two weeks after the symposium. All registered attendees will receive an email notification once the proceedings are available.

SPEAKER DONATION

In lieu of Speaker Gifts, a donation has been made to the Wounded Warrior Project. For additional information, please visit: www.woundedwarriorproject.org.

SURVEY

A survey will be e-mailed to you after the event. NDIA would greatly appreciate your time in completing the survey to help make our event even more successful in the future.

SYMPOSIUM CONTACT

Ms. Brant Murray
Meeting Planner, NDIA
(703) 247-2572
bmurray@ndia.org

EXHIBITS CONTACT

Ms. Allison Hitchner
Exhibits Manager, NDIA
(703) 247-2573
ahitchner@ndia.org

3:00 PM – 3:30 PM

Networking Break in Exhibit Area
Commonwealth North, Cavalier

3:30 PM – 5:00 PM

Panel: Border Security
Commonwealth South

Since 9/11 the control of our Borders has taken on unprecedented importance in ensuring the security of our Nation. This effort requires the daily combined and integrated work of numerous operational law enforcement agencies, the intelligence community, and in some cases, the U.S. military. The challenge of securing 19,937 miles of land border and coastline can seem overwhelming, except for the fact that this integration of efforts is in fact working, albeit always open to challenge and always in need of improvement. Assembled experts will discuss their agency's current and ongoing efforts to address the daunting issue of Border Control.

Moderator: Mr. Mike Becraft, Senior Vice President, Federal Civilian Services, Serco, Inc.

- Mr. Michael J. Fisher, Chief, U.S. Border Patrol, U.S. Department of Homeland Security
- Vice Admiral David Pekoske, USCG (Ret), Executive Vice President, A-T Solutions, Inc.; former Vice Commandant, U.S. Coast Guard
- Mr. Jay Ahern, Principal, The Chertoff Group; former Deputy Commissioner, U.S. Customs & Border Protection

5:00 PM – 6:30 PM

Evening Networking Reception in Exhibit Area
Commonwealth North, Cavalier
(hosted beer and wine)

WEDNESDAY, SEPTEMBER 29, 2010

7:00 AM – 3:00 PM

Registration
Assembly Foyer

7:00 AM – 8:00 AM

Continental Breakfast
South Lobby

8:00 AM – 8:10 AM

Introductory Remarks
Commonwealth South

Mr. Rich Cooper, Principal, Catalyst Partners, LLC; Chairman, NDIA Homeland Security Division

8:10 AM – 8:45 AM

Industry Keynote Address
Commonwealth South

The Honorable Michael Chertoff, Founder & Principal, The Chertoff Group; former Secretary, U.S. Department of Homeland Security

8:45 AM – 9:30 AM Government Keynote Address
Commonwealth South

Mr. Andy Purdy, Chief Cybersecurity Strategist, Computer Sciences Corporation; former Acting Director, National Cyber Security Division/US-CERT, U.S. Department of Homeland Security

9:00 AM – 1:30 PM Exhibit Area Open
Commonwealth North, Cavalier

9:30 AM – 10:00 AM Networking Break in Exhibit Area (Last Chance to View Exhibit Area)
Commonwealth North, Cavalier

10:00 AM – 11:00 AM Panel: Cyber Threats and Enhancing Security of the IT Infrastructure
Commonwealth South

The assembled cyber security leaders will review the status of the existing and emerging threats to the nation's IT infrastructure. They will share architectural and technological approaches to combat the cyber threat and examine ongoing IT infrastructure projects around DHS and how these have contributed to the enhancement of security as well as the need for public and private sector collaboration.

Moderator: Mr. Ben Gianni, Vice President, Homeland Security, Enforcement, Security and Intelligence Division, Computer Sciences Corporation

- Mr. Paul Beckman, CISSP, Chief Information Security Officer (CISO), Information Technology Security Office Risk Management Division, HQ, Office of the Chief Information Officer (CIO), U.S. Department of Homeland Security
- Mr. Scott Charbo, Vice President, Accenture; former Chief Information Officer, U.S. Department of Homeland Security
- Mr. David Wiley, Chief Technology Officer, L-3 Corporation, STRATIS

11:00 AM – 12:15 PM Panel: Critical Infrastructure Protection and Resilience
Commonwealth South

Assessing risk for Critical Infrastructure Protection requires understanding the threat, the impact on the continuity of critical functions and services, interdependencies involved, and the ability to return to normalcy. Once known, this information allows decision-makers to apply limited resources to achieve physical and operational resilience. The alternative is general, unfocused protection. How is this prioritization taking place and how are impacts being measured?

Moderator: Ms. Sue Armstrong, Office of Infrastructure Protection, U.S. Department of Homeland Security

- Mr. Brian Kamoie, Senior Director of Preparedness Policy, Office on Resilience, National Security Council, The White House
- Mr. Paul Molitor, Senior Industry Director, Smart Grid and Strategic Initiatives for the National Electrical Manufacturers Association (NEMA)
- Ms. Yazmin Seda-Sanabria, Senior Program Manager, Critical Infrastructure Protection & Resilience (CIPR) Program Office of Homeland Security, HQ, U.S. Army Corps of Engineers

12:15 PM – 1:30 PM Networking Lunch in Exhibit Area (Last Chance to View Exhibit Area)
Commonwealth North, Cavalier

1:30 PM Exhibit Area Closed

NDIA EVENTS

Please visit the NDIA website for a complete listing of the events we offer.

NDIA website:

<http://www.ndia.org>

Select:

Meetings & Events

Schedule of Events

ADVERTISING

Advertise in *National Defense* magazine and increase your organization's exposure. *National Defense* will be distributed to attendees of this event, as well as other NDIA events. For more information, please contact Dino Pignotti, NDIA, at (703) 247-2541 or dpignotti@ndia.org.

1:30 PM – 3:00 PM

Panel: Covering Risk and Disasters

Commonwealth South

Regardless of when a disaster or emergency occurs, how that event is covered by the media will have a tremendous impact upon political leaders, community residents and the national psyche. From the first broadcast images, information gathering and confusion/ "fog of war" that often occurs, how reporters and new-media bloggers interpret these happenings will shape the response and recovery to the incident. Seasoned journalists will share their insights on covering local and national emergencies and share lessons learned to help prepare for future incidents.

Moderator: Mr. David Olive, Principal, Catalyst Partners, LLC

- Ms. Jeanne Meserve, Homeland Security Correspondent, CNN
- Mr. Rich Esposito, Senior Investigative Reporter, ABC News
- Ms. Donna Leinwand, Reporter, USA Today

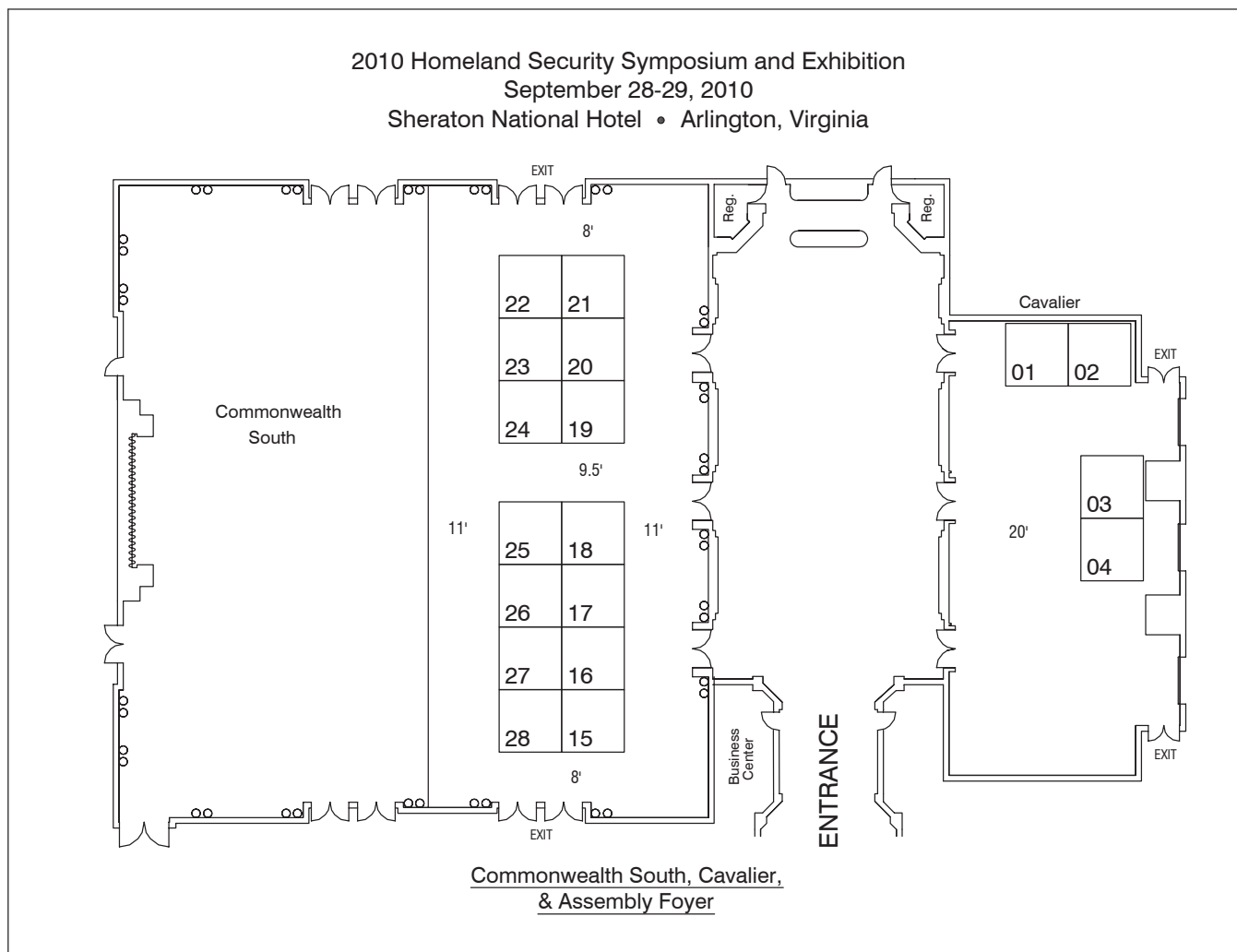
3:00 PM

Conference Wrap-up & Adjournment

Commonwealth South

Mr. Rich Cooper, Principal, Catalyst Partners, LLC; Chairman, NDIA Homeland Security Division

EXHIBITS



Aberdeen Test Center	23	L-3 STRATIS	16
ASRC Primus	20	Lessons Learned Information Sharing	28
Cavalier Logistics	26	Management and Training Consultants, Inc.	24
Department of Homeland Security	4	PENTAX Imaging Company	25
DHS Science & Technology Directorate	1	SiloSmashers	27
DHS Science & Technology Directorate	2	Strategic Solutions Unlimited, Inc.	3
DHS/NCS	18	The Centech Group, Inc.	17
Emergent	15	University of Maryland University College	19
Gerber Legendary Blades	21	University of Phoenix	22

Exhibiting As

Booth

EXHIBITORS

ABERDEEN TEST CENTER

Booth# 23

Defense and Sustainment. Vulnerability testing, Blasts and Blasts effects, Explosive Detection Technology, vehicle emissions and fire suppression.

ASRC PRIMUS

Booth# 20

ASRC Primus offers a full range of IT services to a broad range of Federal and State agencies, as well as commercial clients specializing in Software Engineering disciplines.

CAVALIER LOGISTICS

Booth# 26

Cavalier Logistics is a Veteran owned and operated organization that provides mission critical logistics and transportation solutions to the U.S. Government.

DEPARTMENT OF HOMELAND SECURITY

Booth# 4

The Department's Office of Infrastructure Protection (IP) leads the coordinated national program to reduce risks to the nation's critical infrastructure to strengthen national preparedness, promote rapid recovery and response.

DHS SCIENCE & TECHNOLOGY DIRECTORATE

Booth# 1 and 2

The DHS Science and Technology Directorate, in partnership with National Laboratories such as Sandia National Lab, universities, the private sector and other government agencies helps push the innovation envelope and drive technology development to make the nation safer. www.DHS.gov

DHS/NCS

Booth# 18

The NCS provides priority telecommunications services, coordination, information sharing operations, and other related programs to support National Security and Emergency Preparedness (NS/EP) efforts across Federal, state, and local government, critical infrastructure industry, and other authorized NS/EP organizations under all circumstances, including crisis, disaster, emergency, or attack, from awareness through recovery.

EMERGENT

Booth# 15

Emergent is an IT solution provider focused on solving complex business and mission challenges on behalf of government, commercial, education and healthcare organizations.

GERBER LEGENDARY BLADES

Booth# 21

A global leader in the development of innovative, mission-essential gear including knives, tools, lights and equipment for 70 years. We develop high quality, combat proven products driven by the needs of the modern military.

L-3 STRATIS

Booth# 16

LESSONS LEARNED INFORMATION SHARING

Booth# 28

Lessons Learned Information Sharing (LLIS.gov) is the national, online network of lessons learned, best practices, and innovative ideas for the emergency response and homeland security communities. Sponsored by the U.S. DHS FEMA.

MANAGEMENT AND TRAINING CONSULTANTS, INC.

Booth# 24

Management and Training Consultants, Inc. (MTCI) is a Woman-Owned Business that provides value-added support in the areas of logistics, personnel support, training, recruiting, and technology solutions.

PENTAX IMAGING COMPANY

Booth# 25

PENTAX has provided precision optical solutions since 1919. Pentax Atmospheric Interference Reduction (PAIR) technology allows long-range, real-time video surveillance through fog, snow, sand and other atmospheric phenomena. See what's REALLY there!

SILOSMASHERS

Booth# 27

SiloSmashers delivers powerful best practice methodologies that transform government agencies into successful Peak Performance® enterprises. With SiloSmashers as the catalyst, your agency will aspire, achieve and surpass all barriers.

STRATEGIC SOLUTIONS UNLIMITED, INC.

Booth# 3

Strategic Solutions Unlimited is a Service Disabled Veteran Owned Small Business specializing in all things intelligence, including services, training, and risk and security expertise.

THE CENTECH GROUP, INC.

Booth# 17

THE CENTECH GROUP, Inc. (CENTECH) has been a proven, successful provider of systems and solutions on over 4,000 federal government contracts/task orders and 150 mission critical software development projects. Operating under the principles of Trust, Quality, Service and Value, CENTECH is International Organization for Standardization (ISO) 9001:2008 certified and Capability Maturity Model Integration (CMMI) Maturity Level 3 appraised. Our industry leading management approach has earned CENTECH a stellar reputation and leadership position. CENTECH is determined to fulfill all of our commitments with the highest level of dedication and integrity. We support these fundamental business practices and performance objectives with a complete and written, 100% customer satisfaction performance guarantee on all our products and services, ensuring our clients excellent results.

UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE

Booth# 19

University of Maryland University College, a global leader in adult education, provides career-advancing programs in homeland security and cybersecurity. For information, visit www.umuc.edu.

UNIVERSITY OF PHOENIX

Booth# 22

Professional development and continuing education within CM/DM.

KEYNOTE SPEAKERS

MS. CARYN A. WAGNER



Ms. Caryn A. Wagner was confirmed on February 11, 2010 as the Under Secretary for Intelligence and Analysis at the Department of Homeland Security.

Ms. Wagner served as an instructor in Intelligence Community management for The Intelligence and Security Academy, LLC from October 2008 to October 2009. She retired from the House Permanent Select Committee on Intelligence (HPSCI) on October 1, 2008, where she served as Budget Director and cyber security coordinator. Prior to that, Ms. Wagner served in the Office of the Director of National Intelligence (DNI) as an Assistant Deputy Director of National Intelligence for Management and the first Chief Financial Officer for the National Intelligence Program (NIP). She accepted this position after serving as the Executive Director for Intelligence Community Affairs from April 2004 until May 2005. In that capacity, she was responsible for the Community Management Staff, which provided strategic planning, policy formulation, resource planning, program assessment and budget oversight for the Intelligence Community.

Ms. Wagner's previous position was that of the senior Defense Intelligence Agency (DIA) Representative to Europe. She served as the Director, DIA's liaison to the United States European Command (EUCOM) and to the North Atlantic Treaty Organization (NATO) from April 2003 to April 2004. From October 2000 until April 2003, Ms. Wagner served as DIA Deputy Director for Analysis and Production. The Directorate consisted of approximately 2,000 personnel charged with providing high-quality, all-source military intelligence analysis support to the Combatant Commands and deployed U.S. and allied forces; the Chairman, Joint Chiefs of Staff; and the Secretary of Defense. Ms. Wagner was also the Production Functional Manager, responsible for orchestrating analysis and production by analytic elements of the Services, the Combatant Commands, other defense agencies, and the Commonwealth.

Prior to being appointed the Deputy Director for Analysis and Production, Ms. Wagner headed the Director, Military Intelligence (DMI) Staff from November 1996 to November 2000. In this position, Ms. Wagner conducted military intelligence community planning and was responsible for development and management of the General Defense Intelligence Program (GDIP). She served as an associate member of the Military Intelligence Board (MIB) and oversaw the MIB secretariat. She also managed the implementation of the Joint Intelligence Virtual Architecture (JIVA), a defense intelligence community-wide collaborative environment and tool set.

Prior to her position as the DMI Staff Director, Ms. Wagner was the Staff Director of the Subcommittee on Technical and Tactical Intelligence, House Permanent Select Committee on Intelligence. Her responsibilities included oversight of all technical collection and processing capabilities in the National Intelligence Program (then the NFIP) and Military Intelligence Program (then JMIP and TIARA). Ms. Wagner also served as a member of the Program and Budget Authorization Subcommittee of the House Permanent Select Committee on Intelligence, overseeing the GDIP and national and defense counterintelligence programs.

Prior to working on the HPSCI staff, Ms. Wagner was an associate at Booz Allen Hamilton, working in the areas of Tactical Exploitation of National Capabilities (TENCAP), support to military operations, intelligence planning, and intelligence systems architecture development. Ms. Wagner also served as a Signals Intelligence and Electronic Warfare Officer in the United States Army.

Ms. Wagner received a Bachelor of Arts degree in English and History from the College of William and Mary, and a Master of Science degree in Systems Management from the University of Southern California.

THE HONORABLE MICHAEL CHERTOFF



As Secretary of the U.S. Department of Homeland Security from 2005 to 2009, Mr. Chertoff led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. His greatest successes have earned few headlines – because the important news is what *didn't* happen.

At Chertoff Group, Mr. Chertoff will provide high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery. “Risk management has become the CEO’s concern,” he says. “We help our clients develop comprehensive strategies to manage risk without building barriers that get in the way of carrying on their business.”

Before heading up the Department of Homeland Security, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism – including the investigation of the 9/11 terrorist attacks.

Mr. Chertoff is a *magna cum laude* graduate of Harvard College (1975) and Harvard Law School (1978). From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

In addition to his role at Chertoff Group, Mr. Chertoff is also senior of counsel at Covington & Burling, LLP, and a member of the firm’s White Collar Defense and Investigations practice group.

MR. ANDY PURDY



In early 2007, Mr. Andy Purdy formed DRA Enterprises, Inc., specializing in information assurance and cyber security, software assurance, business development, and government relations. Mr. Purdy provides services as an independent consultant focusing on business strategy, business development, and technology ventures.

Mr. Purdy recently completed work as a Special Government Employee on the Defense Science Board Task Force on the Foreign Influence on Software Development.

Mr. Purdy served as the nation’s “cyber security czar” for two years in his role as Acting Director of the National Cyber Security Division/US-CERT of the Department of Homeland Security. He served in this capacity until October 2006, and was followed by Greg Garcia, appointed as Assistant Secretary for Cyber Security and Telecommunications. Mr. Purdy served for three and a half years at DHS beginning with his role in the set up and launch of the NCSD beginning in April 2003 after he moved to DHS from the White House staff. He

served as Deputy Director through October 2003, after which he served as a Visiting Scientist at the Software Engineering Institute of Carnegie Mellon working fulltime in a contractor capacity supporting DHS/NCSD, until September 2004 when Secretary Ridge appointed him Acting Director, where he served for 24 months. Until the end of December Mr. Purdy served as a Visiting Scientist at the Software Engineering Institute of Carnegie Mellon, working on the Resiliency Engineering Framework with the Financial Services Technology Consortium.

Prior to beginning his work in support of DHS, Mr. Purdy served as a member of the White House staff as Deputy to Howard Schmidt, the Vice Chair of the President’s Critical Infrastructure Protection Board (PCIPB), where he helped to draft the *National Strategy to Secure Cyberspace*. Previously, at the United States Sentencing Commission he served as Acting General Counsel from November 1999 to January 2001 and was Chief Deputy General Counsel from 1989 until that time.

Mr. Purdy served as a Federal prosecutor in Philadelphia, Special Counsel to the House Ethics Committee, Counsel to the Senate Impeachment Trial Committee, and Assistant Attorney General in Missouri. He also worked as Senior Staff Counsel to the House Select Committee on Assassinations’ investigation of the assassination of President Kennedy. He served for five years in network news in Washington at NBC and CBS News.

Mr. Purdy is a graduate of the College of William and Mary and the University of Virginia Law School, and is a member of the bar in the District of Columbia, Maryland, Missouri, and Pennsylvania.

PANELISTS

(In order of appearance)

International Terrorism - The Threat from Abroad

MR. RICH COOPER

Mr. Richard “Rich” Cooper is a Partner with Catalyst Partners, LLC, (formerly known as Olive, Edwards & Cooper, LLC) a government and public affairs practice in Washington, D.C., that focuses on homeland and national security matters. In this role, Mr. Cooper offers client advice and strategic planning support on matters relating to emergency preparedness and business continuity leadership, public-private partnerships, homeland security policies and programs as well as science and technology development and deployment. He also serves as the Vice Chairman of the Homeland Security Division of the National Defense Industrial Association (NDIA); as a member of the American National Standards Institute’s Homeland Security Standards Panel (ANSI-HSSP); and as an Advisor to the Reform Institute and New York University’s International Center for Enterprise Preparedness (InterCEP). He has been featured on Fox News, C-Span, Congressional Quarterly, Government Executive and other media outlets. He posts regular commentaries / ‘Blogs’ on a variety of homeland security issues at Adfer’s Security Debrief.

MR. ROBERT CRUZ

Mr. Robert Cruz is the Product Head for Hiscox Property Terrorism Underwriting in the United States. This also includes the associated lines of Terrorism Liability, War and Political Violence. Mr. Cruz sets the strategic vision for the U.S. regarding risk appetite, rates, and overall staff direction. Robert evaluates security, political events, threats and financial climate in determining suitable risks to underwrite and their related rates. Mr. Cruz manages a book of business that includes iconic building such as the Empire State Building, the New York Stock Exchange, municipalities and small private business.

MS. TINA W. GABBRIELLI

Ms. Tina W. Gabbrielli is the Director of the Office of Risk Management and Analysis (RMA), National Protection and Programs Directorate, at the U.S. Department of Homeland Security. Her office leads the Department’s efforts to develop, implement and share a common framework to address the overall analysis and management of homeland security risk. Prior to her current position, Ms. Gabbrielli was the Senior Director for Contingency Planning and Field-Based Preparedness in the National Preparedness Task Force at the U.S. Department of Homeland Security.

MR. JOHN P. WOODS

Mr. John P. Woods currently serves as the Deputy Assistant Director of Homeland Security Investigations (HSI) at Immigration & Customs Enforcement (ICE). In this capacity Mr. Woods oversees the National Security Investigations Division. As Chief of this 350 person headquarters division, he manages a \$131 million budget and oversees ICE’s investigative, regulatory, and technological programs targeting transnational national security threats arising from illicit travel, trade, and financial enterprises.

MR. BEN TUCKER

Mr. Ben Tucker is a Senior Vice President and the property specialized risk group leader within Marsh’s National Property Practice. Located in the New York office, he is responsible for the coordination and placement of Specialized property products, including standalone terrorism, Global Supply Secure

and WindX parametric wind insurance for Marsh client advisory offices in the U.S. This role entails marketing both new and renewal accounts, and working closely with Marsh servicing offices to provide innovative property insurance solutions, new product development, and benchmarking data.

Domestic Terrorism – The Threat at Home

MR. BILL CARROLL

Mr. Bill Carroll is the Senior Vice President of Strategic Programs at SiloSmashers and has over thirty-five years of extensive experience in Operational Management and Program Management within Homeland Security, the Federal Law Enforcement Community, and the Intelligence Community, and State and Local Law Enforcement agencies. He has provided expert consultation services on business Strategy and Operational/ Program management to Fortune Five Hundred Companies.

MR. BRIAN DODD

Mr. Brian Dodd, Chief, Counter-Narcoterrorism Operations Center (CNTOC), Special Operations Division (SOD), he serves as DEA’s lead spokesperson on extraterritorial investigations against the leaders of major drug trafficking organizations and terrorist networks. Mr. Dodd is an expert on drug trafficking and the growing threat of narco-terrorism, as the nexus between drug trafficking organizations and terrorist groups becomes more evident.

MR. AKMAL ALI

Mr. Akmal Ali represents the Office of SAFETY Act Implementation (OSAI), Science and Technology Directorate, Department of Homeland Security. The mission of OSAI is to provide incentives to industry to develop and deploy effective anti-terrorism technologies and services to the maximum extent possible. Mr. Ali’s work in OSAI includes his previous work as an economic evaluator, and his current role dealing with legal issues and coordination of the SAFETY Act with various government agencies and industry sectors.

The Wrath and Consequences of “Mother Nature”

THE HONORABLE NANCY HARVEY STEORTS

The Honorable Nancy Harvey Steorts has had a distinguished career in business and trade, political service, academia, journalism and real estate. President Ronald Reagan appointed her Chairman of the U.S. Consumer Product Safety Commission. Prior to that she was a consultant to the Director of the U.S. Office on Consumer Affairs at the White House and earlier served as Special Assistant for Consumer Affairs to the Secretary of Agriculture under the Nixon and Ford administrations. She was President of the prestigious Dallas Citizens Council, an organization of Chief Executive Officers of the major corporations; was named “one of the Best Public Servants” by the Gallagher Report; and was awarded the George P. Arents Medal for Excellence in Government by her alma mater, Syracuse University – the highest award given to an alumna.

MS. LAURA K. FURGIONE

Ms. Laura K. Furgione is the National Oceanic and Atmospheric Administration (NOAA) Deputy Assistant Administrator for Weather Services and Deputy Director of the National Weather Service (NWS). In this role, she is responsible for the day-to-day civilian weather operations for the United States, its territories, adjacent waters and ocean areas.

LIEUTENANT REX STRICKLAND

Lieutenant Rex Strickland is an 18-year veteran of the Fairfax County (VA) Fire & Rescue Department. He is currently assigned to one of four Heavy Rescue Squads responsible for Technical Rescue operations in Fairfax County, as well as around the DC region. Additionally, he serves as an Operations Chief for the department's Urban, Search, & Rescue Task Force, commonly referred to as Virginia Task Force One. Lieutenant Strickland has deployed with the US&R team over a dozen times to include the Embassy Bombing in Nairobi, Kenya; The Pentagon response; Earthquakes twice in Turkey, Taiwan, and Iran; Hurricane responses such as Katrina and several stand-by events. He was the primary Operations Chief for the Haiti earthquake. His primary background is with rescue operations; however, he has a wide variety of training in Technical Search operations, long-term planning, and Incident Command. He is a Structural Collapse Technician lead instructor for DHS/FEMA.

MR. CHARLES SHIMANSKI

Mr. Charley Shimanski joined the American Red Cross in 2008 and currently serves as Senior Vice President of Disaster Services at the Red Cross national headquarters in Washington, D.C. In this role, Mr. Shimanski co-leads a team of 180 dedicated staff nationwide, and nearly 90,000 registered volunteers providing disaster response throughout the United States.

MR. CHRISTOPHER ROYSE

Mr. Christopher "Chris" Royse is currently the Senior Program Director for Global Threat Reduction and Security Initiatives for Parsons Infrastructure & Technology. Mr. Royse provides program management for Parsons Cooperative Threat Reduction Integration Contract and is responsible for building Parsons portfolio of global projects in support of proliferation prevention and U.S. national security objectives. Most recently, Mr. Royse was responsible for establishing Parsons support of USAID's Project Management Unit in Port Au Prince Haiti for the recovery and reconstruction efforts following the January 12, 2010 earthquake there.

Border Security

MR. MIKE BECRAFT

Mr. Mike Becraft leads the Federal Civilian Services Group, an organization consisting of three major business units with over 4,000 personnel providing direct support to federal, provincial, and state and local governments in the United States and Canada. Prior to joining Serco, Mr. Becraft was the Executive Vice President for Mission Services at SI International where he had previously served as the Senior Vice President for Homeland Security. Prior to joining SI International he served for 10 years in the United States Immigration and Naturalization Service (INS) starting first as an Expert Consultant in October 1993. In February 1995 he was appointed Chief of Staff as a member of the Career Senior Executive Service. On September 11, 2001 he was appointed Acting Deputy Commissioner. His last major responsibility was to lead the restructuring and transition of the agency from the Department of Justice into the Department of Homeland Security. He is the recipient of the Presidential Meritorious Rank Award for 2002. Mr. Becraft also served a career in the U.S. Army.

CHIEF MICHAEL J. FISHER

On May 9, 2010, San Diego Sector Chief Patrol Agent Michael Fisher was named Chief of the U.S. Border Patrol after Chief David Aguilar became the Deputy Commissioner of CBP. Chief Fisher started his duty along the Southwest Border in 1987 in Douglas, AZ. He successfully completed the selection process for the Border Patrol Tactical Unit (BORTAC) in 1990 and was later selected as a Field Operations Supervisor for the tactical unit, assigned to El Paso, TX for four years. In that capacity, Chief Fisher planned and executed operations throughout the United States and in nine foreign countries. Following this he also served as the Deputy Chief Patrol Agent in the Detroit Sector and as an Assistant Chief Patrol Agent in Tucson, AZ. During the transition to the Department of Homeland Security in March of 2003, he was assigned as the Deputy Director for U.S. Customs and Border Protection's Office of Anti-Terrorism in Washington, D.C. In this capacity, he staffed and directed the office during periods of increased threat and was CBP's liaison to the inter-agency intelligence community for anti-terrorist planning and operations coordination. Chief Fisher then served in Border Patrol headquarters before being assigned back to the field in February of 2006 as the Deputy Chief in San Diego Sector. He was promoted to Chief Patrol Agent of San Diego Sector in June of 2007.

VICE ADMIRAL DAVID P. PEKOSKE, USCG (RET)

Vice Admiral David P. Pekoske, USCG (Ret), is the Executive Vice President of A-T Solutions, Inc. where he is responsible for developing and managing A-T Solutions' expanding international maritime and port security business units. Prior to joining A-T Solutions, VADM Pekoske was the Vice Commandant of the United States Coast Guard where he served as the second in command and the Chief Operating Officer responsible for executing the Commandant's strategic intent, managing internal organizational governance and as the Component Acquisition Executive.

THE HONORABLE JAYSON P. AHERN

On January 2, 2010, Mr. Jayson P. Ahern retired from 33 years of federal service to both the U.S. Customs Service and U.S. Customs and Border Protection. At the time of his retirement, he had served for nearly a year as Acting Commissioner of U.S. Customs and Border Protection (CBP) and was responsible for securing, managing and controlling our Nation's borders.

Cyber Threats and Enhancing Security of the IT Infrastructure

MR. BEN GIANNI

Mr. Ben Gianni is the Operations Executive responsible for his company's performance on projects with the U.S. Department of Homeland Security (DHS). He also serves as the CSC Program Manager for the DHS Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE) contract. Since joining CSC in 1983, Mr. Gianni has specialized in managing IDIQ programs and complex, multi-agency integration projects involving cyber security, data centers, telecommunications networks and a variety of software engineering and development projects associated with transportation, homeland security, health, human services, economic development, public safety and other aspects specific to state and federal government. Mr. Gianni is a certified Project Management Professional. He has a bachelor's degree in industrial engineering from the University of Pittsburgh and a master's degree in computer science from the Johns Hopkins University.

MR. PAUL G. BECKMAN

Mr. Paul G. Beckman is the Chief Information Security Officer for the Headquarter Component of DHS and the Director of the Information Technology Services Organization (ITSO) Risk Management Division. He joined the DHS OCIO as the Branch Chief of Information Security in November 2005. His Division's primary responsibilities include Enterprise IT Security, COMSEC and Configuration Management. Prior to his assignment at DHS, Mr. Beckman spent 5 years at the Pentagon, providing support to the HQ Department of Army under the Pentagon Network Infrastructure Division as their Information Assurance Manager. Mr. Beckman holds several certifications as a CISSP, CCNA, MCSE MCSA, CWNA, and CWSP. He received his Bachelors of Science from Radford University.

MR. ROBERT G. WILLIAMS

Mr. Robert G. Williams serves as the Director of the Data Center Branch of the DHS Office of Chief Information Officer IT Services Division. In this role he leads and manages the DHS Program to Develop and Operation Enterprise Wide Data Centers and migrate DHS Systems and Capabilities into these Facilities. Prior to his service at DHS, Mr. Williams held various roles in the corporate IT world, including Director of Network Operations at America Online, Vice President of Network Deployment at Rhythms DSL where he deployed over 800 DSL colocations, and was responsible for Local Market Switched Network Delivery services at MCI Telecommunications. Mr. Williams also served as a commission officer in the U.S. Navy on several surface combatants, and holds a BS Degree in Engineering from the Pennsylvania State University.

MR. SCOTT CHARBO

Mr. Scott Charbo is the Vice President for Cyber Security and Telecommunications at Accenture Federal. Previously, he was the Deputy UnderSecretary for the National Protection and Programs Directorate (NPPD) at DHS, where he was lead for the Comprehensive National CyberSecurity Initiative. He also served as CIO for DHS and UnderSecretary for Management. His focus as CIO was establishing a reliable, secure infrastructure to support the information sharing and work of the department. Mr. Charbo also served as CIO for USDA from 2003-2005. Mr. Charbo, was President of mPower3, Inc., a subsidiary of ConAgra Foods, where his business was assurance systems and modeling for food integrity. When not working, you will find him with his family.

MR. DAVID WILEY

Mr. David Wiley is the Chief Technology Officer for the L-3 Corporation, STRATIS. STRATIS is a >\$1B division providing intelligence and information systems solutions to federal, state and local government agencies. He has more than 29 years of continuous experience across the information technology systems lifecycle for multiple application domains. Mr. Wiley has been the contractor program manager for three large U.S. government programs including research, development and testing of advanced space systems. Currently, he leads L-3 STRATIS products and services offered to clients in areas of secure cloud computing delivery, IT services and expertise location through internal knowledge management programs. He holds certifications in program management and systems engineering.

Critical Infrastructure Protection and Resilience**MS. SUE ARMSTRONG**

Ms. Sue Armstrong was named the Acting Deputy Assistant Secretary of the Office of Infrastructure Protection (IP) on September 18, 2009. In this capacity, she oversees the day to day management and administration of IP, and all Infrastructure Protection programs within the National Protection and Programs Directorate on behalf of the Assistant Secretary for Infrastructure Protection. Prior to that, she served as the Director of the Infrastructure Security Compliance Division (ISCD) of IP beginning in June 2008, and was named the Director, ISCD in January 2009. In this capacity, she was responsible for the program implementing the Chemical Facility Anti-Terrorism Standards regulations, which went into effect in June 2008. From December 2005 until June 2008, she served as IP's Deputy Chief of Staff, and then Chief of Staff. From May 2003 until coming to IP, Ms. Armstrong served as the Deputy Chief of Staff of the Information Analysis and Infrastructure Protection Directorate of the Department.

MR. BRIAN KAMOIE

Mr. Brian Kamoie is Senior Director of Preparedness Policy on the White House National Security Staff. In this role he leads the development of national policy related to all-hazards preparedness, individual and community resilience, domestic critical infrastructure protection and resilience, preparedness grants and national security professional development. Before joining the White House National Security Staff, Mr. Kamoie served as Deputy Assistance Secretary for Preparedness and Response and Director of the Office of Policy, Strategic Planning and Communications at the U.S. Department of Health and Human services (HHS). In this role, he led efforts in policy development, strategic planning and communications related to preparedness for and response to bioterrorism and other public health emergencies.

MR. PAUL A. MOLITOR

Mr. Paul A. Molitor serves as the Senior Industry Director of Smart Grid and Strategic Initiatives for the National Electrical Manufacturers Association in Rosslyn, VA. On behalf of the 450 member companies of NEMA, Mr. Molitor is responsible for monitoring the national Smart Grid effort and interfacing with electric utilities, manufacturers, federal agencies, and the U.S. Congress on Smart Grid issues. He also provides information, direction, and support to the NEMA Government Relations, Technical Services, and Industry Operations groups who manage policy and technical issues related to standards and protocols for U.S. and International Smart Grid activities. Mr. Molitor is the Plenary Secretary of the NIST Smart Grid Interoperability Panel (SGIP), and is active in the NIST cybersecurity coordinating task group and the International Electrotechnical Commission Strategy Group 3 (IEC SG3) on Smart Grid. He is also a member of the IEEE Power & Energy Society and the IEEE Standards Association, and is a standards development representative to the Canadian Task Force on Smart Grid Technologies and Standards (TF-SGTS). Mr. Molitor has had several Smart Grid articles published in U.S. and International publications, is a core member of the Gridweek and Grid-Interop Organizing Committees, and is a member of the editorial board for ElectroIndustry Magazine.

MS. YAZMIN SEDA-SANABRIA

Ms. Yazmin Seda-Sanabria is native of Mayagüez, Puerto Rico. She earned a Bachelor of Science degree in Civil Engineering from the University of Puerto Rico at Mayagüez in 1991. She also earned a Master of Engineering degree in Civil Engineering from the same university in 1994. Subsequently, she earned a Master of Science degree in Engineering Mechanics from Mississippi State University in 1998. Ms. Seda-Sanabria has also completed the Department of the Army's Intern Leadership Development course and Army Management Staff College Basic Course. In 1994, she joined the

U.S. Army Engineer Waterways Experiment Station – now U.S. Army Engineer Research and Development Center (ERDC) – as a research structural engineer in the Structural Mechanics Division, Structures Laboratory. In 2006 Ms. Seda-Sanabria joined the U.S. Army Corp of Engineers (USACE), Headquarters Office as Senior Program Manager in the Directorate of Civil works, Office of Homeland Security, where she is responsible for providing guidance and overseeing USACE program development, defense, and execution of the Critical Infrastructure Protection and Resilience (CIPR) Program. In this role, Ms. Seda-Sanabria oversees the development and implementation of a national risk management strategy for the protection, security, and improved resilience of the USACE portfolio of critical dams, navigation locks, and levee systems. Throughout her career, Ms. Seda-Sanabria has received numerous annual performance awards and letters of commendation.

Covering Risks and Disasters

MR. DAVID M. OLIVE

Mr. David M. Olive has more than 30 years of experience in business, politics, law and public affairs. As former Chief of Staff to U.S. Rep. Asa Hutchinson (R-AR3) and a former staffer for U.S. Senator Jim Allen (D-AL). Mr. Olive understands that very few things get done in Washington without approaching them in a bi-partisan manner. In 2005, The Hill named Mr. Olive one of the top Homeland Security lobbyists in Washington, D.C. He established and currently serves as the moderator of The Washington Homeland Security Roundtable and is a frequent contributor to Security Debrief, a homeland security blog.

MS. JEANNE MESERVE

Ms. Jeanne Meserve is CNN's Washington, D.C.-based Homeland Security Correspondent. In this role, Ms. Meserve has covered a wide-range of stories, including Guantanamo Bay, security during President Barack Obama's inauguration, Hurricane Katrina and September 11, 2001. Meserve played a key role in CNN's Peabody award-winning coverage of Hurricane Katrina, providing the first reports of devastating flooding in New Orleans. Judges for the 2005 David Bloom Award gave Meserve special recognition, saying her coverage revealed "extraordinary composure and compassion as well as her unwavering respect for the facts." Ms. Meserve also provided reports for two CNN Security Watch specials: "Is America Prepared? Lessons of Hurricane Katrina" and "Is America Prepared? The Next Disaster." Covering homeland security since the September 11, 2001 attacks, Ms. Meserve has reported on security of the nation's ports, chemical plants, airports and borders. She has flown with a federal air marshal, accompanied a combat air patrol in an F-16 and stood atop a 13-story crane in the Port of Los Angeles.

MR. JOHN D. SOLOMON

Mr. John D. Solomon edits a blog on public preparedness, In Case Of Emergency, Read Blog (www.incaseofemergencyblog.com). He is the author of a forthcoming book, In Case of Emergency, Read Book: Preparing You, Your Family and Your Community For Natural Disasters, Terrorism, Pandemics, and Other Threats Of The 21st Century. Mr. Solomon is a correspondent with the NPR show, "On The Media" where he has reported on homeland security, disasters and the press. Mr. Solomon is an Adjunct Instructor in Emergency Medicine at the State University of New York College of Medicine. He is a member of New York City's Citizen Emergency Response Team (CERT) Program and is a volunteer with the American Red Cross of Greater New York. Mr. Solomon was selected as the "Ready New Yorker of the Month" by the City of New York's Office of Emergency Management.

MR. RICHARD J. ESPOSITO

Mr. Richard Esposito is the Senior Investigative Reporter for ABC News. A journalist with more than 25 years of newspaper and television experience, his news gathering career began in 1977 when he was hired as a copy boy at the New York Daily News. He is a winner of the 2005 George Polk Award for Television Reporting as a result of his ABC News investigation into the CIA's network of secret prisons and the intelligence agency's harsh interrogation techniques as well as a 2006 Emmy Award for Investigative Reporting. In addition he shares in a 2007 Peabody Award for Investigative Journalism. At ABC News, Mr. Esposito's focus is Homeland Security, National Security and the complex issues of the nation's criminal justice system.

MS. DONNA LEINWAND

Ms. Donna Leinwand is a reporter covering the Justice Department, major crimes, legal issues, disasters and terrorism at USA Today, the nation's largest circulation daily newspaper. Her reporting assignments have taken her to Hamburg, Germany in the path of the 9/11 terrorists, Jerusalem in the wake of suicide bombings, Baghdad to cover the war, Indonesia and Thailand after the tsunami and London during the subway bombings. She has covered more than 20 hurricanes, including Andrew, Katrina, Ike, Ivan, Isabel, Jeanne, Georges, Gustav, Alberto and Frances. She most recently traveled to Haiti to cover the earthquake that struck outside Port-au-Prince.

ATTENDEE ROSTER

Dr. Marianne Abbott
The MITRE Corporation

Mr. Michael Adams
Naval Surface Warfare Center-Panama City

Mr. Jay Ahern
The Chertoff Group

Mr. David Aimone
Buchanan, Ingersoll and Rooney, PC

Mr. Akmal Ali
DHS, S&T

Dr. KP Ananth
Idaho National Laboratory

Mr. Robert Andreas
Thales USA Defense

Mr. George Appley, III
Concurrent Technologies Corporation

Mrs. Sue Armstrong
DHS, Office of Infrastructure Protection

Mr. Dan Arnold
Harris Corporation

Dr. Thomas Austin
The Boeing Company

Mr. Steve Baker
Parsons

Ms. Lolita Baldor
Associated Press

Mr. Erik Ballinger
Alliant Techsystems

Mrs. Lisa Barr
DHS

MG Barry Bates, USA (Ret)
NDIA

Mr. Joe Beal
Creative Computing Solutions, Inc.

Mr. Paul Beckman
DHS, CIO

Mr. Mike Becraft
Serco, Inc.

Mr. Mike Benz
NORC at the University of Chicago

Mr. Brian Berry
Aberdeen Test Center

Mrs. Carlaine Blizzard
EADS North America

Mr. David Bloom
Kforce Government Solutions

Mr. Tim Bortz
Wilcox Industries Corporation

COL Steve Bucci, USA (Ret)
IBM

Mr. Sean Buckley
Parsons

Ms. Lynda Burroughs
ManTech International Corporation

LCDR Kevin Camp, USCG (Ret)
DCS Corporation

Mr. Vincent Cannava
L-3 Communications

Dr. Curtis Carey
NOAA National Weather Service

Lt Col Lew Carlisle, USAF (Ret)
ITT Space Systems

Mr. Bill Carroll
SiloSmashers

Mr. Steve Cass
Sierra Nevada Corporation

Mr. Mel Chang
Tactical Electronics

Mr. Scott Charbo
Accenture

Hon. Michael Chertoff
The Chertoff Group

Mr. Jeff Chyzik
Naval Inspector General

Mr. Jerry Clark
U.S. GAO

Ms. Machaela Collins
Nuclear Security Services Corp.

Mr. Larry Conner
LMI Government Consulting

Mr. Rich Cooper
Catalyst Partners, LLC

Mr. Dwayne Cormier
Naval Inspector General

Mr. Phil Cormier
The Boeing Company

CAPT Carl Cramb, USN (Ret)
Alion Science and Technology

VADM Terry Cross, USCG (Ret)
EADS North America

Lt Col Gary Cruse, USAF (Ret)
Northrop Grumman

Mr. Rob Cruz
Hiscox International Insurance

Mr. Robert Cunningham
New Zealand Trade & Enterprise

Mr. Gregory Davis
Hazmed, Inc.

Mr. Patrick Dawson
Layer 7 Technologies

Mr. Jay DeCianno
General Dynamics

Mr. Herb Dempsey
ARCADIS

Mr. Larry DeRoche
Vectronix, Inc.

Ms. Laura Dion
Windmill International, Inc.

Lt Col Jeff Ditlevson, USAF
U.S. Transportation Command

Mr. Bernie DiTullio
Cisco Systems, Inc.

Mr. Brian Dodd
Drug Enforcement Administration

Mr. Michael Doyle
Naval Inspector General

Ms. Linda Drake
Applied Signal Technology, Inc.

Mr. Paul Druckman
Accenture

Mr. Dave Duffy
NEK Advanced Securities Group, Inc.

Ms. Hollie Dupes
Jacobs Engineering Group, Inc.

Ms. Sarah Ellis Peed
DHS, Office of Risk Management & Analysis

Mr. Rich Esposito
ABC News

Mr. Micke Everitt
CGI Federal

Ms. Stacie Fain
Teledyne Brown CollaborX, Inc.

Mr. Michael Fisher
U.S. Border Patrol

Mr. Mark Fitzgerald
U.S. Coast Guard Forum

Mr. Jeff Freeman
DRS Technologies, Inc.

Dr. John Frim
Canadian Embassy

Ms. Laura Furgione
NOAA National Weather Service

Ms. Tina Gabbrielli
DHS, Office of Risk Management & Analysis

Mr. Robert Gauthier
Computer Sciences Corporation

Ms. Kim Gavin
BBN

Mr. Ben Gianni
Computer Sciences Corporation

Mr. Jim Gigrich
Agilent Technologies

Ms. Kim Gill
Pyxis, LLC

Mr. Brendan Glasgow
SafeNet, Inc.

Mr. Mark Graves
Jacobs Engineering Group, Inc.

Mr. John Gresham
GS5, LLC

Mr. Joe Guirrerri
PESystems, Inc.

Dr. Bob Hahn, II
Serco, Inc.

Mr. Eric Hakimov
Monument Capital Group, LLC

Mr. James Hanke
Aberdeen Test Center

Ms. Sharon Hardie
General Dynamics

Mr. Eric Harkness
Booz Allen Hamilton

Mr. Mike Harper
Coquina Visions

Maj Gen George Harrison, USAF (Ret)
Georgia Tech Research Institute

Ms. Jenny Hess
U.S. Army-RDECOM, AMRDEC

Col Steve Heuer, USAF (Ret)
U.S. Transportation Command

Mr. Terry Hilderbrand
Georgia Tech Research Institute

Ms. Erin Hoffman
DHS

Mr. Michael Höglund
Saab

Mrs. Bonnie Holt
DHS, National Infrastructure Protection Program

Ms. Ellen Howe
L-3 Communications

LTC Randy Hull, USA (Ret)
DRS Defense Solutions, LLC

Mr. Stephen Hunt
DJC2 JPO

Ms. Billie Huntley
Verizon Wireless

Mr. Travers Hurst
Oak Ridge National Laboratory

Ms. Lynnette Jefferson
The REGER Group

Mr. Ed Jozwiak
The REGER Group

Mr. Brian Kamoie
National Security Council, The White House

Mr. Mike Kelly
Battelle

Mr. Tim Killebrew
Novonics Corporation

Mr Steve Kimmel
Alion Science and Technology

Mr. Gary Knight
Picerne Military Housing

Mr. Ryan Kociolek
Computer Sciences Corporation

Mr. Alan Koenig
Naval Surface Warfare Center-Crane

LCDR Keith Kruse, USN (Ret)
CRA, Inc.

Ms. Brooke Kyle
NetApp

Ms. Victoria Laing
Battelle

Ms. Donna Leinwand
USA Today

Mr. Jeff Lett
Eagle Support Services Corporation

CDR Howie Lind, USN (Ret)
Fluor Enterprises, Inc.

Mr. David Lloyd
Summit Marketing

Mr. Andrew Lluberes
DHS, I&A

Mr. Stephen Lopez
URS Corporation

Mr. Neil Lovering
Intelligent Waves, LLC

Mr. Mark Luker
Vectronix, Inc.

Ms. Leigh McCook
Georgia Tech Research Institute

Mr. John McDowall
MTCSC, Inc.

Mr. Michael McGhee
Raytheon Company

Mr. Jon McIntosh
Booz Allen Hamilton

Dr. Dave McIntyre
National Graduate School

Dr. David McWhorter
Catalyst Partners, LLC

Ms. Jeanne Meserve
CNN

Col Wayne Messner, USAF (Ret)
WKM Security Associates

Mrs. Betty Mills-Carilli
U.S. Border Patrol

Mr. Paul Molitor
National Electrical Manufacturers Association

Mr. Napoleon Montes-Amaya
Hiscox

Mr. Bob Montgomery
L-3 Communications

Mr. Gene Moran
DRS Technologies, Inc.

LCDR Joe Morgan, USCG
Coast Guard Congressional Government Affairs Office

CAPT Lee Moss, USN (Ret)
The Boeing Company

Mr. Chris Munley
Booz Allen Hamilton

Mr. Hugh Murphy
PURVIS Systems, Inc.

Mr. Young Nam
Raytheon Company

Mr. Waseem Naqvi
Raytheon Company

Mrs. Carissa Nee
BAE Systems

Mr. George Nelson
Cole Engineering Services, Inc.

CAPT Jack Nicholson, USN
PMW 146

Mr. Phil Nivens
InfoPro Corporation

Mr. Trevor Odell
BAE Systems

Mr. Strati Oktay
Battelle

Mr. David Olive
Catalyst Partners, LLC

Mr. Dave Paddock
INDUS Corporation

Ms. Sally Pavlow Johnson
NOAA National Weather Service

VADM Dave Pecoske, USCG (Ret)
A-T Solutions, Inc.

Dr. Jeff Piotrowski
Ensco, Inc.

Mr. Joe Pipczynski, Jr.
Telephonics Corporation

Mr. Mike Pizzuto
Research Analysis and Engineering

Mr. Doug Poggi
HMS, Inc.

Mr. Andy Purdy
Computer Sciences Corporation

Mr. Michael Quan
Interactive Tactical Group

Mr. Marcelo Quiroga
Intrexon Corporation

Mr. Cameron Raithel
L-3 STRATIS

CPT Rich Reba, USA (Ret)
Computer Sciences Corporation

Mr. Marc Roberts
SRC, Inc.

Mr. Chad Roney
Naval Surface Warfare Center-Crane

Mr. Don Ross
A-T Solutions, Inc.

Mr. Chris Royce
Parsons

RADM Paul Ryan, USN (Ret)
Whitney, Bradley & Brown

Ms. Ashleigh Sanders
U.S. Department of Homeland Security

Mr. Pat Schambach
Computer Sciences Corporation

Mr. Bradley Schreiber
Applied Science Center for Homeland Security

Mr. Fred Schvien
The Boeing Company

Ms. Yazmin Seda-Sanabria
U.S. Army Corps of Engineers, HQ

Mr. John Severino
IBM

Dr. Shash Shashidhar
Polestar Technologies, Inc.

Mr. Peter Shaw
Parsons

Mr. Ray Sheffield
Naval Surface Warfare Center-Panama City

Ms. Stacey Shepard
Jacobs Engineering Group, Inc.

Mr. Charley Shimanski
American Red Cross

Mr. John Solomon
In Case of Emergency, Read Blog

LTG Edward Soriano, USA (Ret)
Northrop Grumman

Mr. Tim Starkey
Witt Associates

Mr. Mark Steiner
American Council of Engineering Companies

Mr. Kevin Stenstrom
Raytheon Company

Hon. Nancy Steorts
Nancy Harvey Steorts & Associates

Dr. Matthew Stershic
Honeywell International

Ms. Frances Stites
SRC, Inc.

Lt. Rex Strickland
Fairfax Co. Urban Search and Rescue

Mr. Ken Stroeck
Tetra Tech EM, Inc.

CAPT Al Stuart, Jr., USN (Ret)
Serco, Inc.

Mr. Larry Studdiford
Jacobs Engineering Group, Inc.

Mr. Shayne Sullivan
Mettters Industries, Inc.

Mr. Raymond Szymanski
Air Force Research Laboratory

Mr. Durval Tavares
ASFTAUUV

Mr. Mark Telich
U.S. Coast Guard, District 9

Ms. Stephanie Tennyson
DHS

Ms. Kristine Thayer
University of Phoenix

Mr. Lenny Thomas
Accenture

Ms. Ria Thomas
Fabiani & Company

Mr. Rick Thomas
Ensco, Inc.

Mrs. Eileen Trent
Windmill International, Inc.

Mr. Ben Tucker
Marsh, Inc.

Mr. Richard Valerius
GS5, LLC

Mr. Jim VanSice
EADS North America

Ms. Caryn Wagner
DHS, I&A

Mr. Brian Weisman
SPAWAR Systems Center-San Diego

Mr. Todd Westrick
Ericsson Federal, Inc.

Mr. Dave Wiley
L-3 Corporation, STRATIS

Mr. Robert Williams
DHS, CIO

Maj Bob Wood, USAF (Ret)
Teledyne Brown CollaborX, Inc.

Mr. John Woods
ICE, Homeland Security Investigations

Ms. Kelly Woods Vaughn
Wiser Company, LLC

RADM Jerry Woolever, USCG (Ret)
Affiliated Computer Services, Inc.

Mr. Song Yom
ASRC Primus

Mr. Ed Yost
Computer Sciences Corporation

RADM Charlie Young, USN (Ret)
Oceaneering International, Inc.

Ms. Tracy Zack
Hazard Management Solutions

Dr. Hank Zimon
MPRI

AMERICA SECURE AWARD

NOMINATIONS NOW OPEN!

The NDIA Homeland Security Division annually presents its highest award, the America Secure Award, to a deserving individual or organization in recognition of their contributions to making the United States a more secure and prosperous nation. The award ceremony is planned for Winter 2010.

The description of the America Secure Award selection criteria is below. Last year's award recipients were the DHS Department of Homeland Security Customs and Border Protection – specifically:

- Mr. David Aguilar, Acting Commissioner and current Chief of the U.S. Border Patrol
- Mr. Jay Ahern, The Chertoff Group; former Deputy Commissioner, U.S. Customs & Border Protection
- Chief Gustavo “Gus” De La Vina, Former Chief of the U.S. Border Patrol (Posthumous)

Selection Criteria

Recipients of the America Secure Award should:

- Provide exemplary and consistent contributions to the policies, programs or operations associated with the nation's homeland security and homeland defense efforts
- Perform distinguished and meritorious actions that have occurred during challenging circumstances (all-hazards)
- Possess recognized or acknowledged insight, stature and expertise in the areas of security homeland security or homeland defense
- Recognize the valued and critical relationships between the public and private sectors to safeguard the nation's security, innovation, entrepreneurship and civil rights/civil liberties
- Exhibit extraordinary leadership and service capabilities consistent with the ideals of American people and its Constitution.

Names sent in for nomination will be shared with the entire Homeland Security Division for consideration prior to voting. Each member of the Division will have one vote.

Nominating Procedure

Please e-mail the name (individual(s) or organization), a biography and contact information for your nominee(s) to:
Mr. Paul Druckman
Chair, America Secure Award Nominating Committee
paul.j.druckman@accenture.com
(571) 205-9055

All nominations will receive a confirmation of receipt. Please be sure to verify that you receive this notification if you submit a nomination. All nominations will be collected and forwarded to the NDIA Homeland Security Division Chair for Division consideration.

Nominations will close on October 8, 2010.

SPONSORS



Accenture is a global management consulting, technology services and outsourcing company. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. With more than 190,000 people serving clients in more than 120 countries, the company generated net revenues of U.S. \$21.58 billion for the fiscal year ended August 31, 2009. For more information, please visit: www.accenture.com.



Emergent is an IT solution provider focused on solving complex business and mission challenges on behalf of government, commercial, education and healthcare organizations. The Emergent team combines unmatched IT technical expertise and an extensive knowledge of the government procurement process. We work hand-in-hand with a variety of complementary IT vendors to ensure our customers receive world class IT solutions, enabling them to achieve their objectives on time and on budget. Emergent's extensive partner network allows our customers to access a multitude of pre-competed, pre-negotiated contracts that deliver a smooth, streamlined procurement experience. For more information, please visit: www.emergent360.com.

This image shows a single page of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page, leaving small margins at the top and bottom. There are no vertical margin lines or other markings on the page.

ARLINGTON, VA
SEPTEMBER 28-29, 2010
WWW.NDIA.ORG/MEETINGS/0490

NOTES

[illegible]

THANK YOU TO OUR SPONSORS!



CATALYST | PARTNERS



Protecting you, Protecting U.S.

SAFETY Act

September 2010

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002

www.safetyact.gov

U.S. DEPARTMENT OF
HOMELAND SECURITY

**Homeland
Security**

Protecting you, Protecting U.S.

SAFETY Act

September 2010

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002

U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

Protecting you, Protecting U.S.

SAFETY Act

September 2010

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002

U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

Protecting you, Protecting U.S.

SAFETY Act

September 2010

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002

U.S. DEPARTMENT OF
HOMELAND SECURITY

**Homeland
Security**



Protecting you, Protecting U.S.

SAFETY Act

September 2010

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002

www.safetyact.gov

U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

A Summary of the SAFETY Act

- The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) was enacted as part of the Homeland Security Act of 2002 (Title VIII, Subtitle G)
- Intended to facilitate the development and deployment of effective anti-terrorism technologies by creating systems of “risk management” and “litigation management”
- Provides important legal liability protections for manufacturers and sellers of technologies and services that could save lives in the event of a terrorist attack
- Protections apply **only** to claims arising out of, relating to, or resulting from an Act of Terrorism



Homeland
Security

What is Eligible for SAFETY Act Protections?

The SAFETY Act liability protections apply to a wide range of technologies, including:

- Products
- Services
- Software and other forms of intellectual property

Examples of eligible technologies:

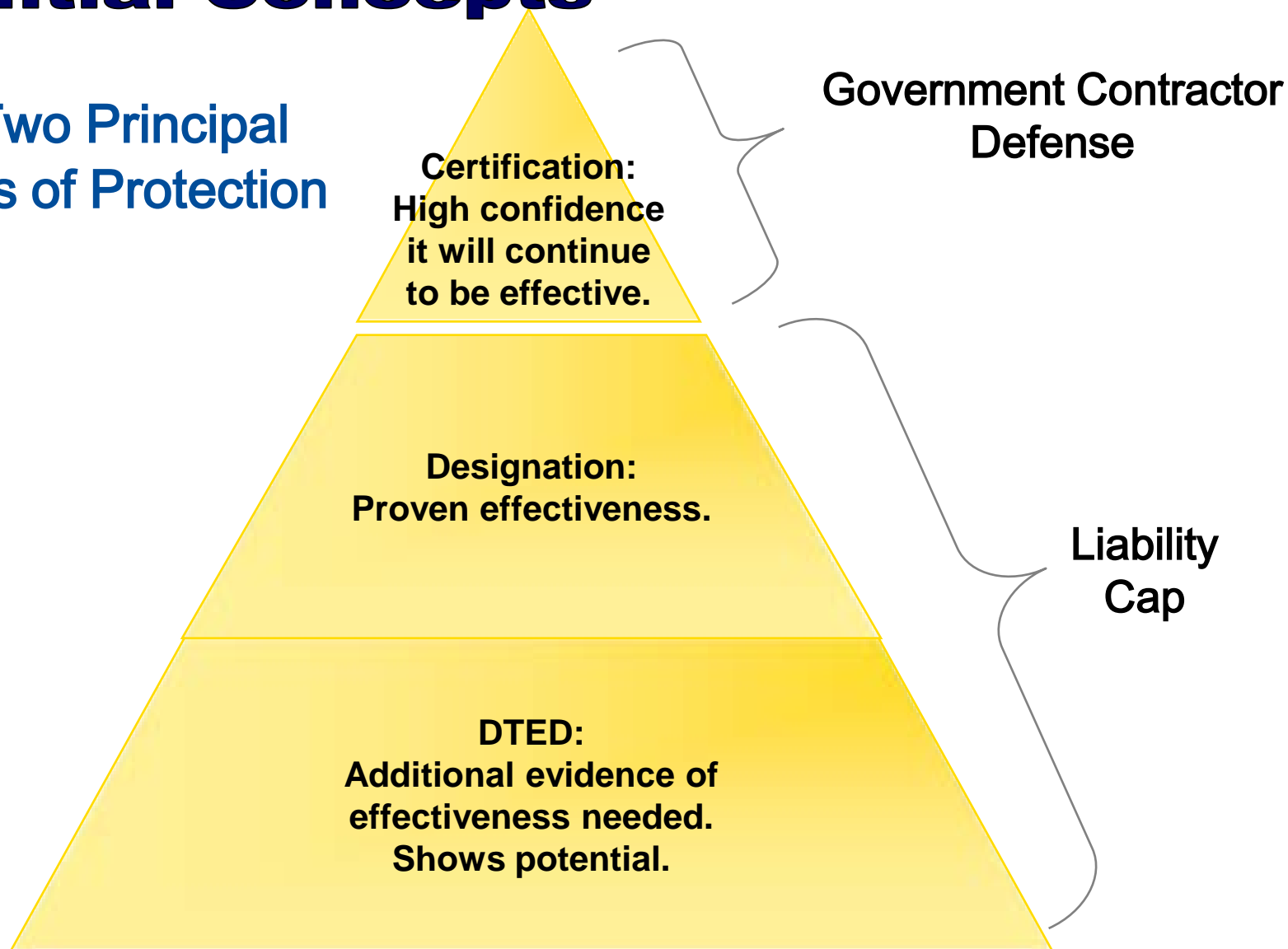
- Threat and vulnerability assessment services
 - Detection Systems
 - Blast Mitigation Materials
 - Screening Services
- Sensors and Sensor Integration
- Threatening Object Detectors
- Decision Support Software
 - Security Services
- Crisis Management Systems
- Cyber Security Technologies



Homeland
Security

Essential Concepts

1. Two Principal Levels of Protection



Homeland
Security

Essential Concepts

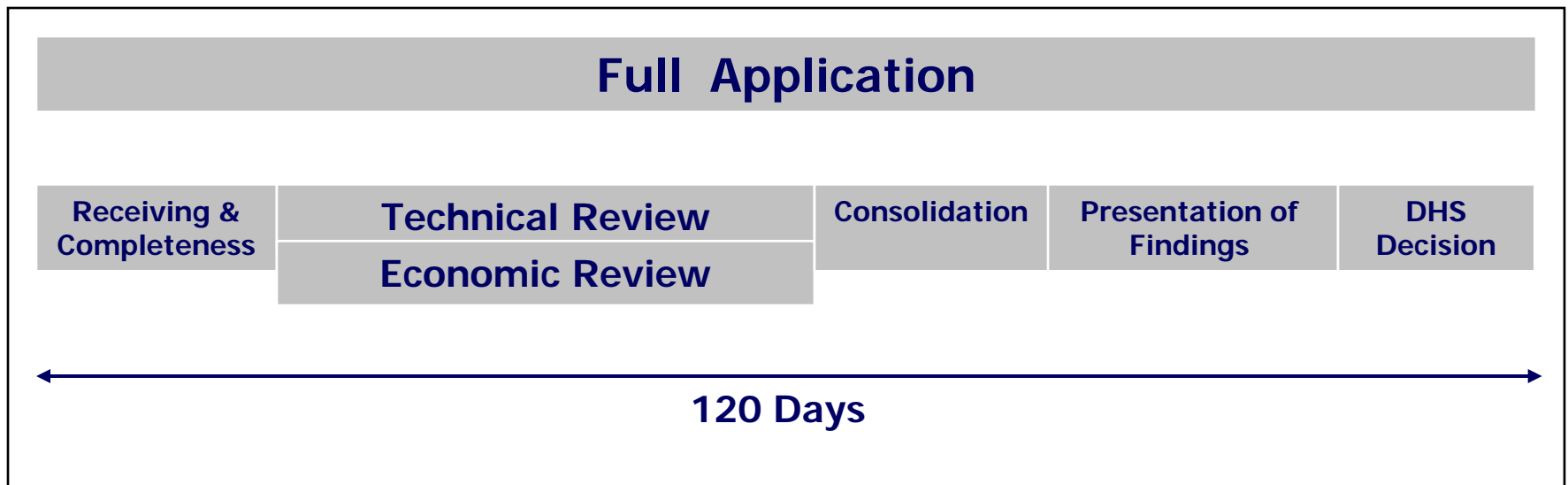
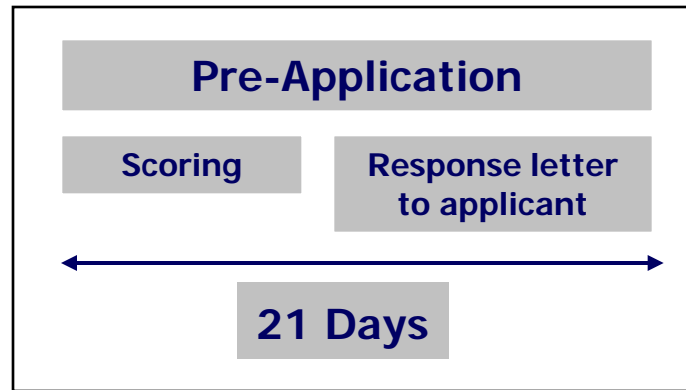
4. SAFETY Act Protections Extend to Users *(whether Designation or Certification)*

“Such cause of action may be brought only against the Seller of the QATT and may not be brought against the buyers, the buyers’ contractors, downstream users of the QATT, the Seller’s suppliers or contractors, or any other person or entity...”

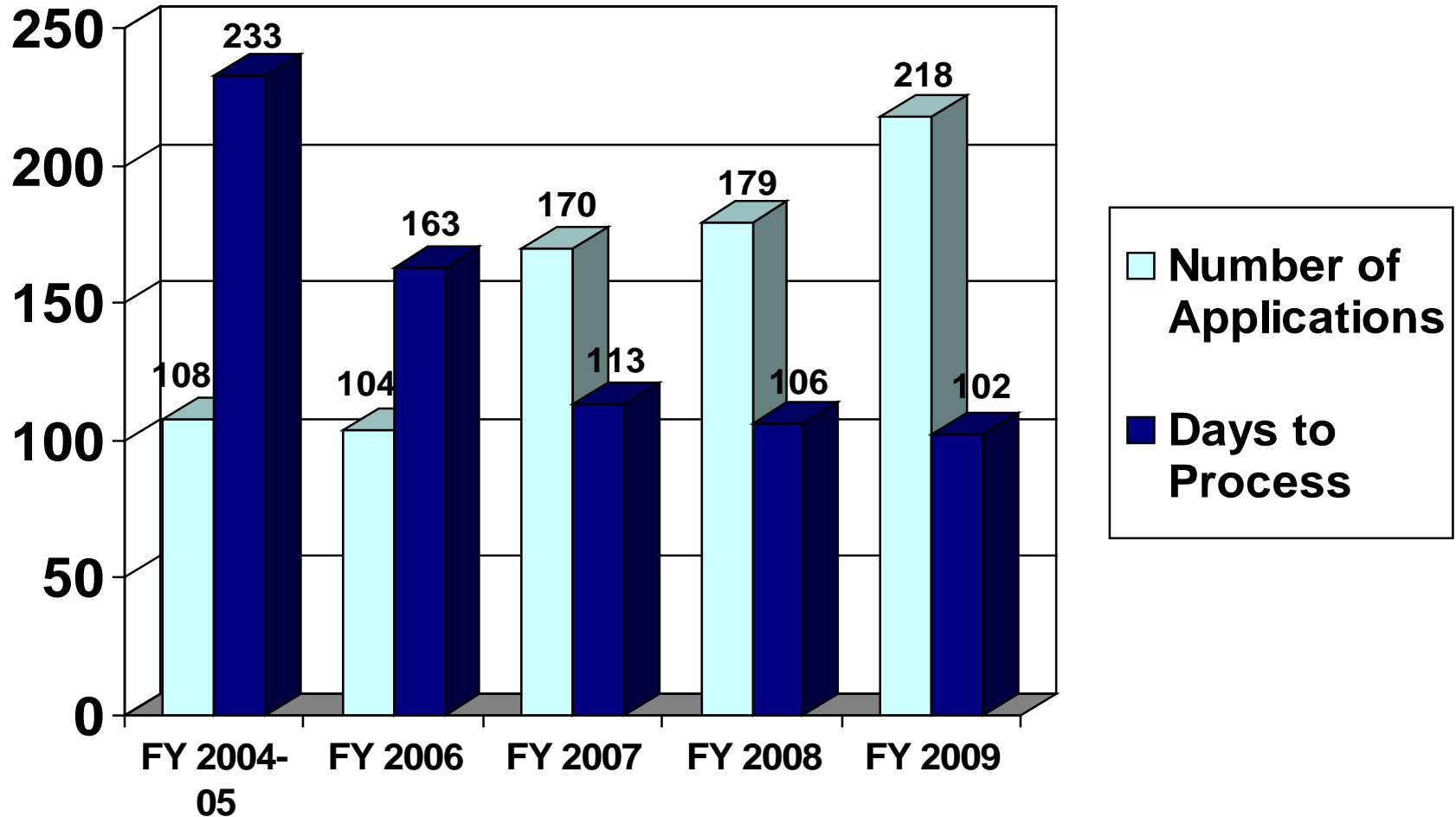
-Preamble to Final Rule, 6 CFR Part 25, at 33150.



Timeline of SAFETY Act Application Review Process

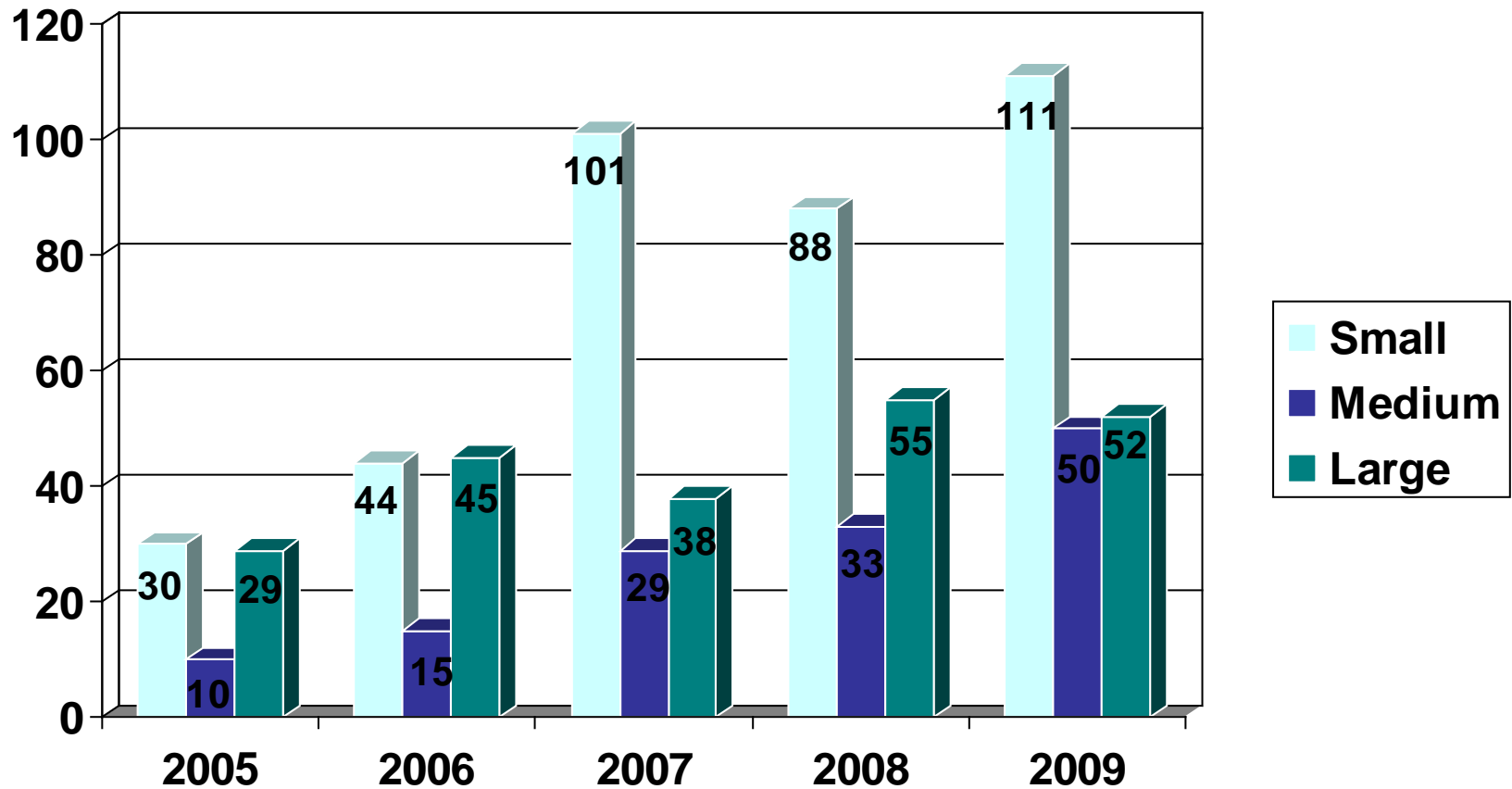


SAFETY Act Progress



Homeland
Security

Applications by Company Size*



*Small = \$0 - \$50,000,000

*Medium = \$50,000,000 - \$1,000,000,000

*Large = Over \$1,000,000,000 by Net Revenue



Homeland
Security

Additional SAFETY Act Information



- Online: www.safetyact.gov
 - FAQs
 - Help Topics
 - Help Desk: Online form for questions requiring an individual response
- Email: helpdesk@safetyact.gov
- Toll-Free: 1-866-788-9318



Homeland
Security



Homeland
Security



DHS Risk Management and Enterprise Datacenter Consolidation

DHS OCIO ITSO



Homeland
Security

What is Risk Management to Me?

What is Risk Management to DHS HQ CISO?

- Complexity is the Arch enemy of Security
 - This includes everything. Processes, systems, infrastructures, security models, etc...*
- There are a myriad of models in a myriad of disciplines
 - At the end of the day, most boil down to: Risk= Probability X Impact.
- Centralized vs. Decentralized Age Old Argument
 - From a Risk Perspective:
 - Decentralized = High Probability/Moderate Impact
 - Centralized = Low Probability/High Impact
- We have (appropriately) come back to Centralization/Consolidation
 - Cost Benefits (Economies of Scale)
 - Manageability = Security



Consolidations = Simplification

- **OneNet (Enterprise Backbone- Ties the Department together)**
- **Enterprise Datacenter Consolidation (Fosters Cloudy capabilities)**
 - E-mail as a Service
 - Blade Technology/Virtualization
 - What else? Anything. Eventually Desktop as a Service
 - “X” as a Service
- **OMB Trusted Internet Connection (Enterprise Internet Connection)**
 - Extranet
 - DMZ
 - Remote Access
- **Benefits: Cost, Security and Simplicity (By rate of comparison)**



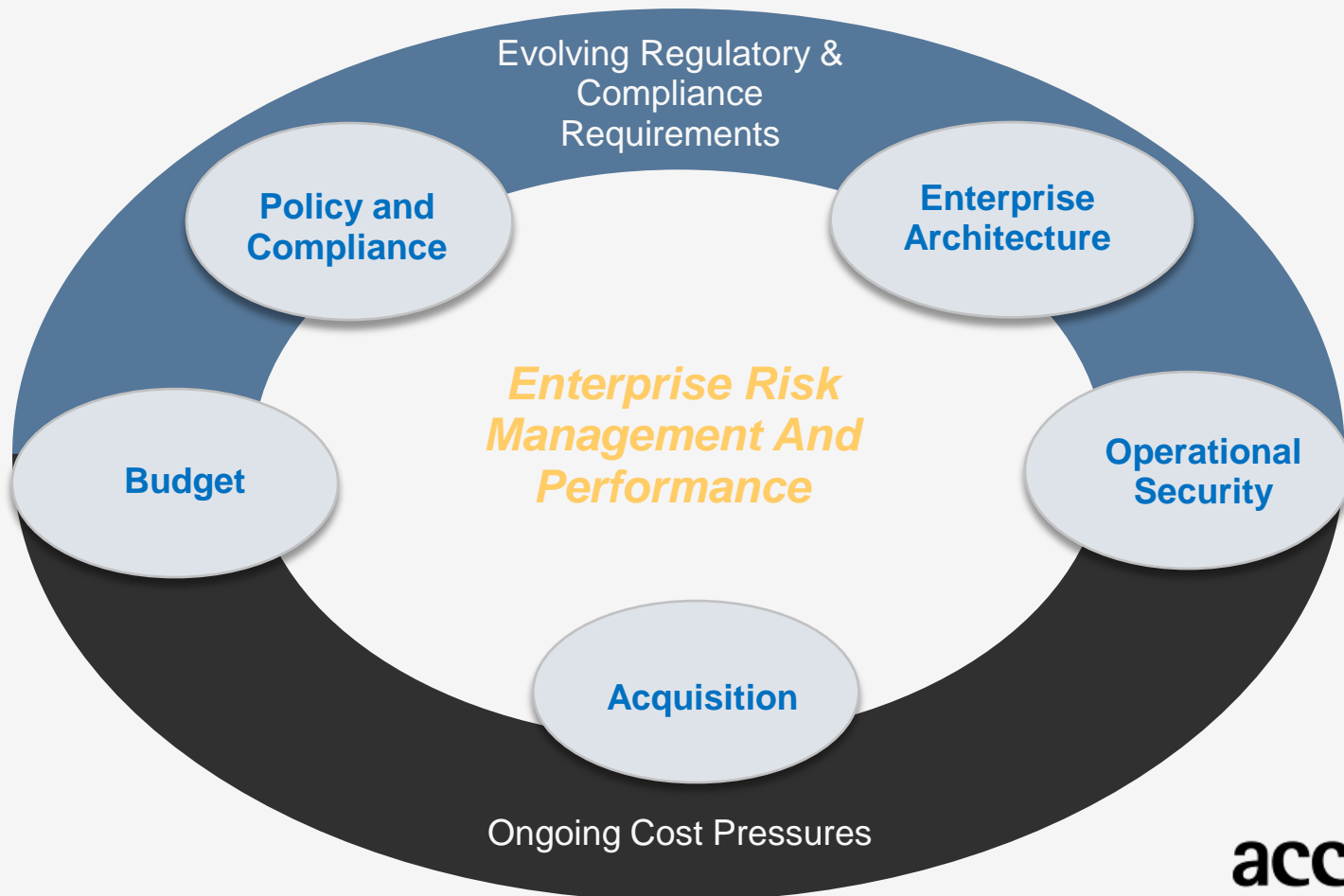


Homeland Security



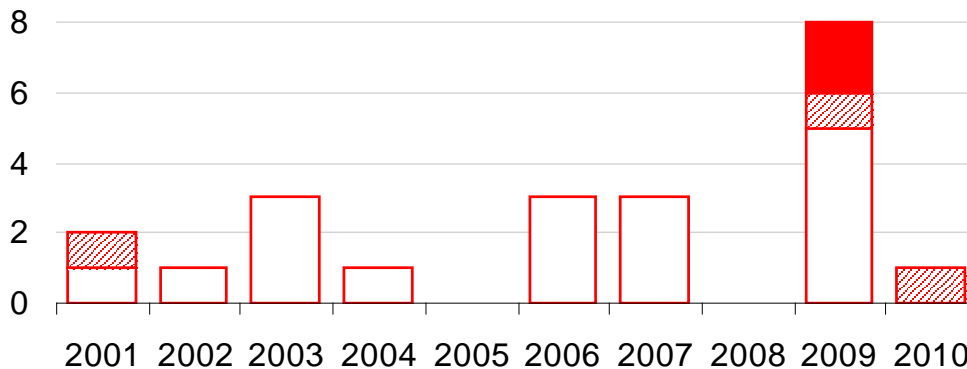
A Risk and Performance Framework that Expands the Security Ecology

Risk decisions cannot be centered around “security” alone. **There are five factors** that should be aligned and coordinated. **Security cannot be viewed in isolation.**



Post-9/11 terrorism against the US

Plots, attempts and attacks against US homeland

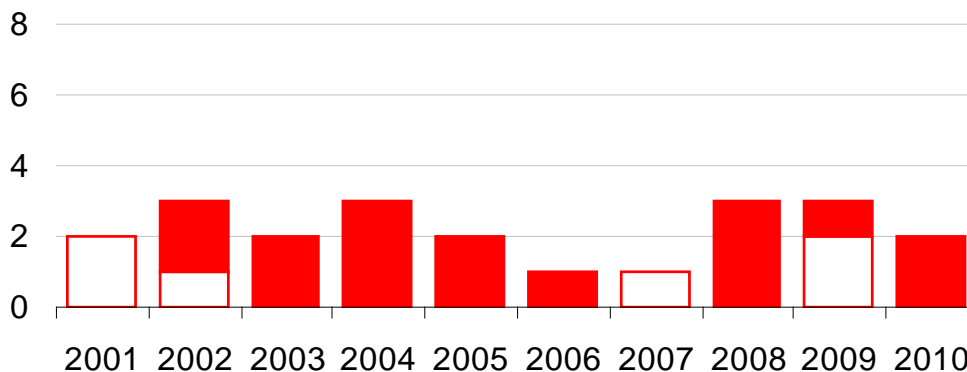


No major transnational terrorist attack on US soil since 9/11 and only minor domestic attacks

Primary domestic targets: aviation, mass transit (esp. NYC subway), iconic structures, military assets

Threat increasingly originates with homegrown radicals

Plots and attacks against US targets abroad



Numerous deadly attacks against American targets abroad

Primary foreign targets: embassies/consulates, hotels, military assets, expat compounds

Threat stems mainly from indigenous militant/insurgent groups

Significant transnational terrorist groups

Al-Qaida core

Al-Qaida in the Arabian Peninsula (AQAP)

Tehrik-i-Taliban Pakistan (TTP)

Mujahideen Al-Shabaab



Major global terrorism incidents since 9/11

2002: Bali/Yemen/Mombasa/
Tunisia

2003: Casablanca/Istanbul/
Philippines

2004: Madrid/Saudi Arabia/
Philippines/Jakarta

2005: London/Bali/Jordan/
Egypt

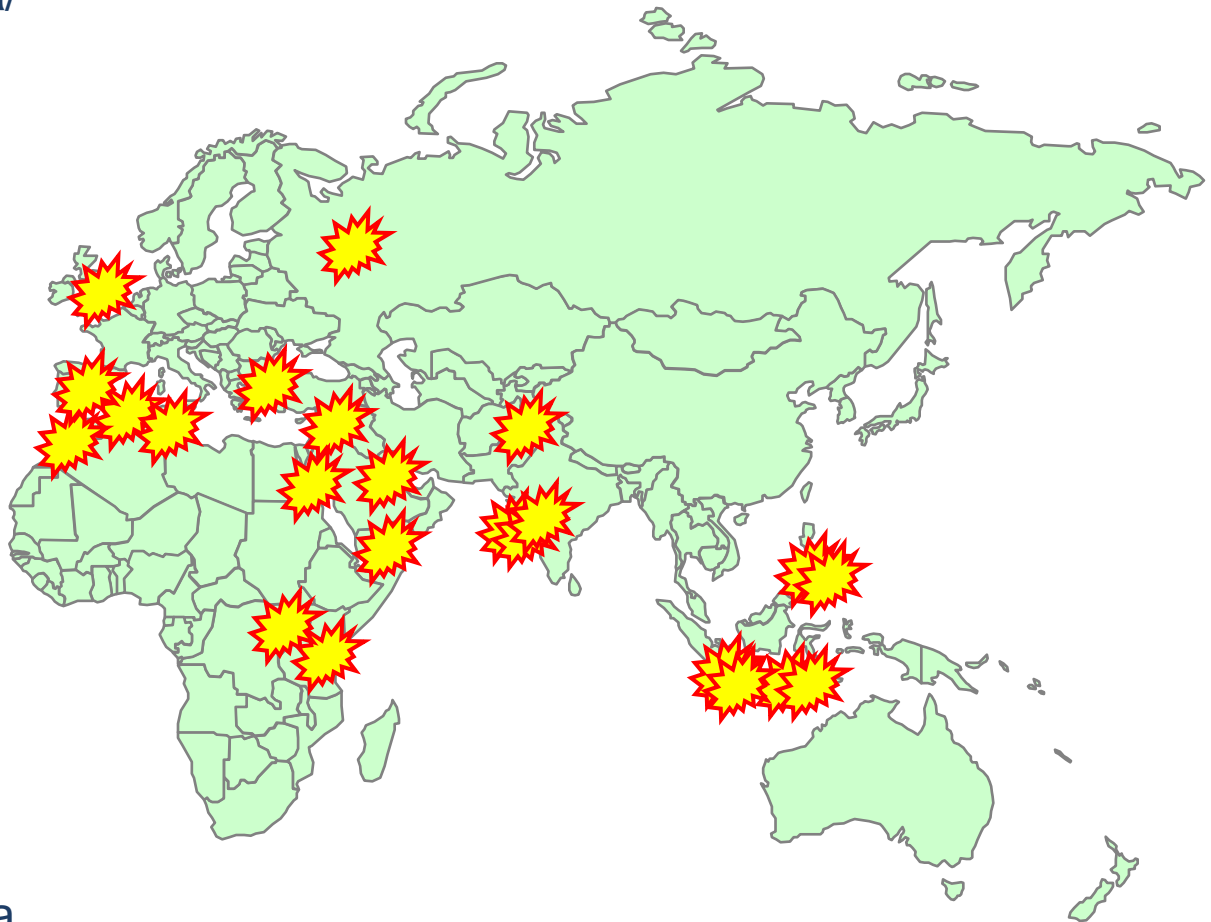
2006: India

2007: Algiers

2008: Mumbai/Islamabad

2009: Jakarta

2010: Moscow/India/Uganda



Terrorism threats stemming from Mexico

- **International terrorist groups** – No permanent or significant presence in Mexico, but could try to enter the US via its southern border.
- **Domestic terrorist groups** – There are two main domestic sources of risk that could potentially carry out a terrorist attack:
 - **Leftist guerrillas** – negligible level of threat to assets within US territory and US-owned assets in Mexico.
 - **Organised crime** – drug-trafficking cartels represent a negligible level of threat to US homeland security, but a low to moderate threat to US-owned assets within Mexico.
- **No evidence of collusion** between drug cartels and terrorist organisations.





U.S. Drug Enforcement Administration

The Nexus Between Drugs and Terrorism



Brian Dodd
Chief

Counter-Narcoterrorism Operations Center
Special Operations Division



Drug Enforcement Administration

- ❖ Single mission agency – enforce U.S. controlled substances laws and regulations
- ❖ Relatively small Federal agency
 - 2009 Budget ~ \$2.6 billion
 - 10,784 employees (5,233 Special Agents)

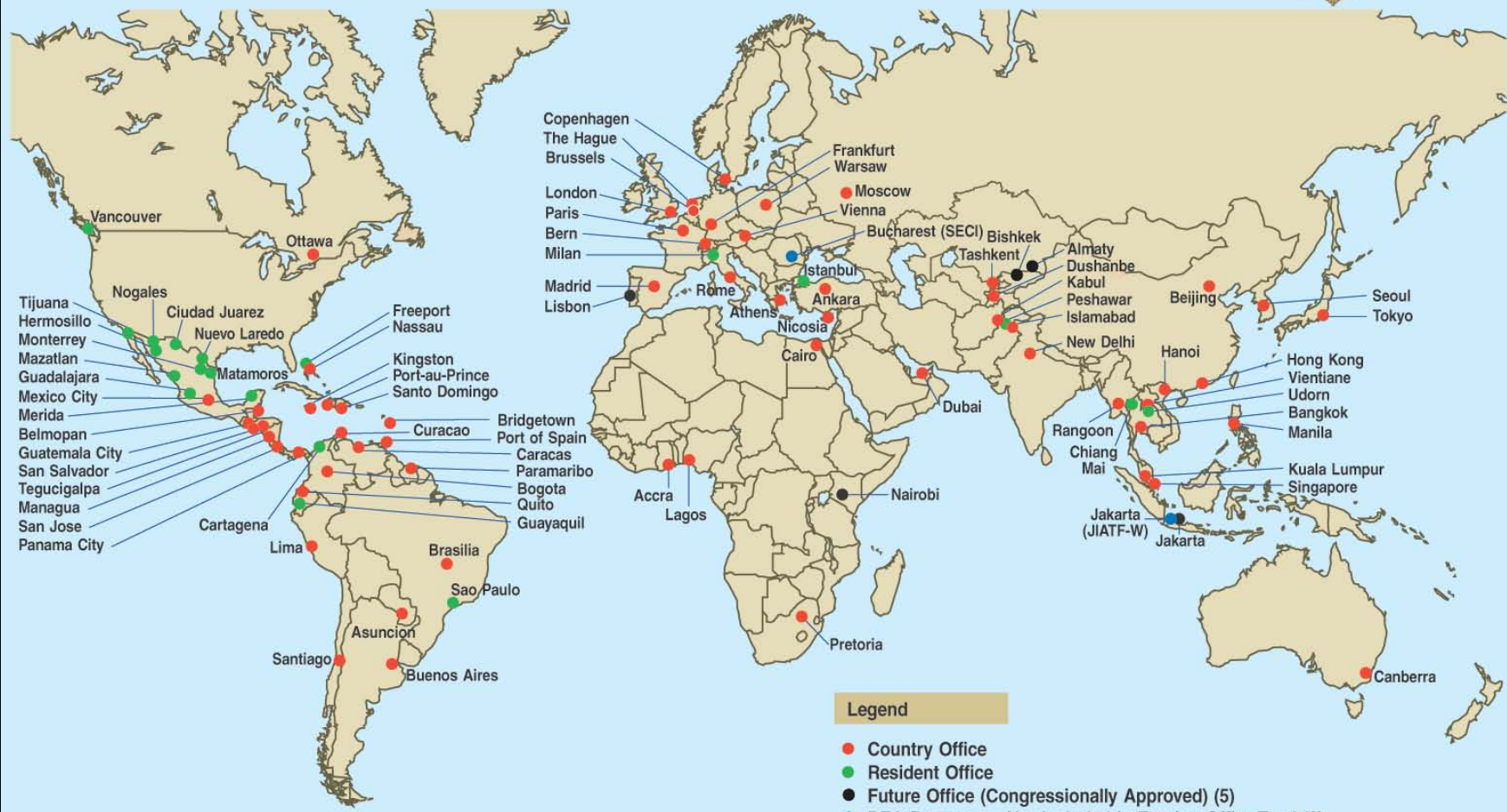




DEA International Presence

DEA Foreign Offices

U.S. Department of Justice
Drug Enforcement Administration



Legend

- Country Office
 - Resident Office
 - Future Office (Congressionally Approved) (5)
 - DEA Presence - Not Included in Foreign Office Total (2)
- 82 Foreign Offices in 61 Countries**



Early Narcoterrorism Definition

❖ “Narcoterrorism” may have been coined in 1983

- Former President Belaunde Terry of Peru used the term to describe terrorist-type attacks against his nation’s anti-narcotics police



❖ “Narco-driven terrorism”

- Drug trafficking organizations that use terrorist tactics (high-profile violence and intimidation) to advance or protect their drug trafficking activities



Colombian Narcoterrorism



Avianca bombing
11/27/89
110 dead



DAS HQ bombing
12/6/89
50 dead / 600 wounded



Modern Narcoterrorism Definition

❖ “Narco-supported terrorism”

- Terrorist / insurgent organizations that use drug trafficking proceeds to advance their political agenda



\$4.7 Million Seized







\$3.57 Million Seizure

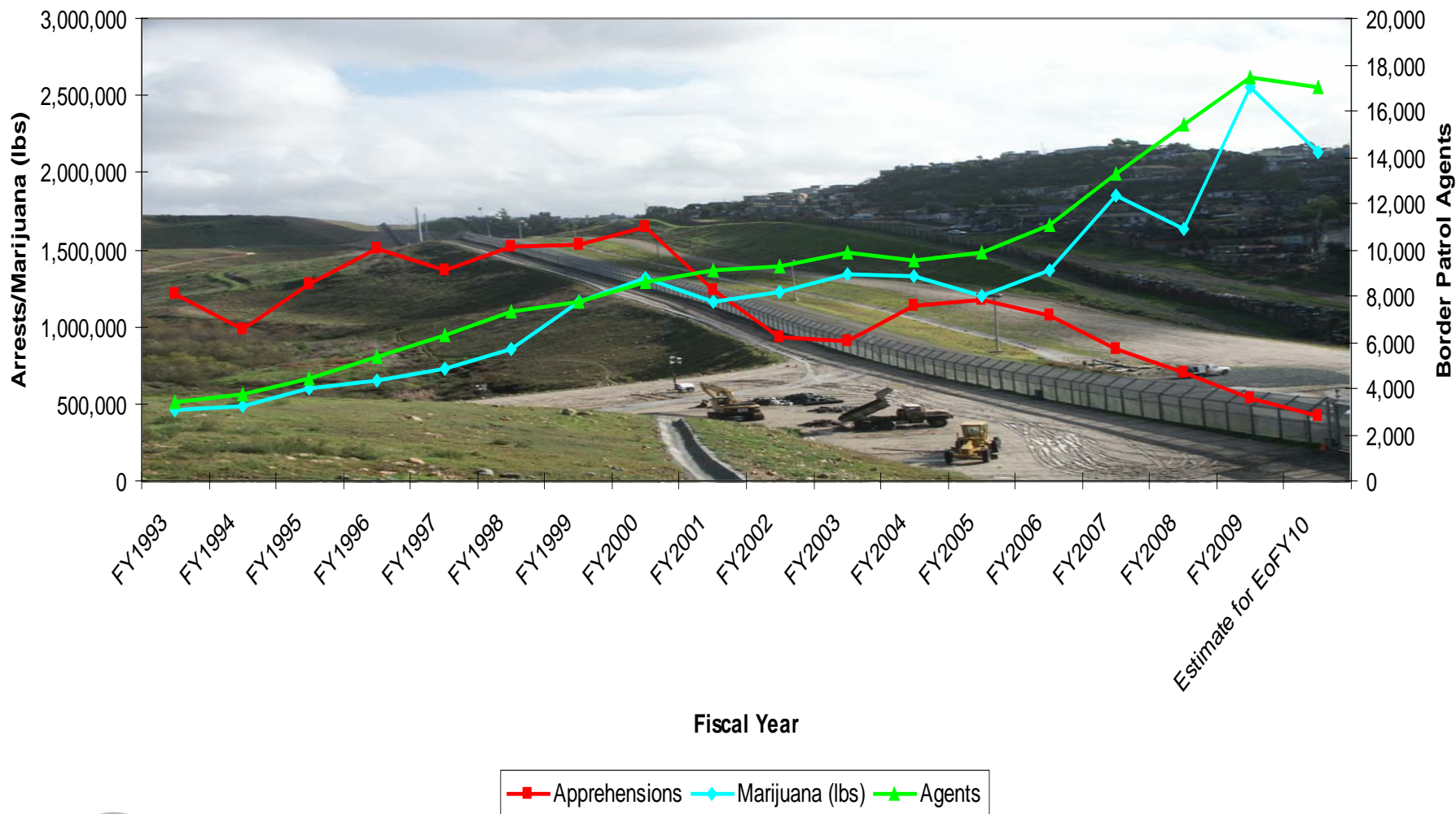




March 2007: \$207 Million



Southwest Border Agents, Apprehensions and Marijuana Seizures FY93-FY10 (Projected)

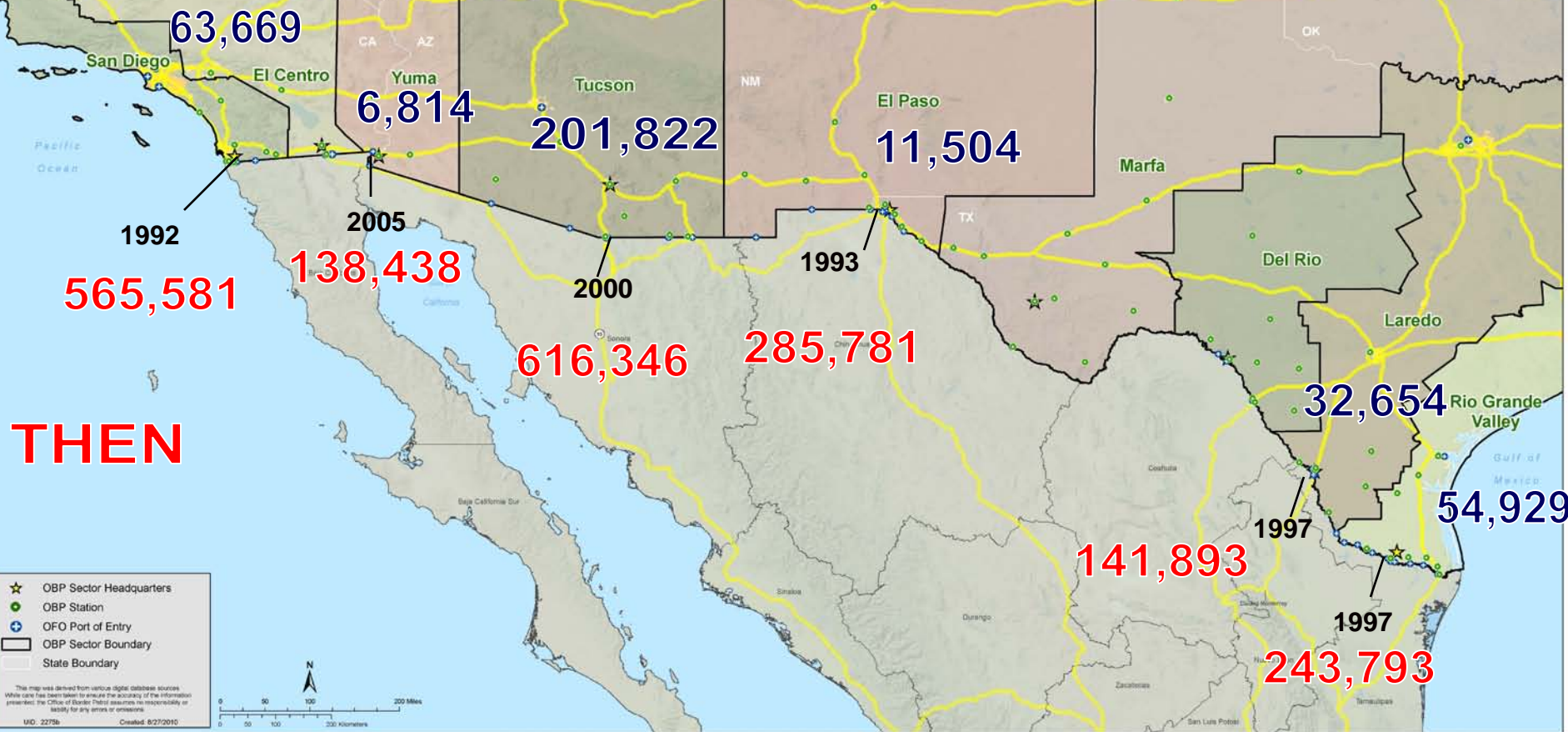


U.S. Customs and
Border Protection



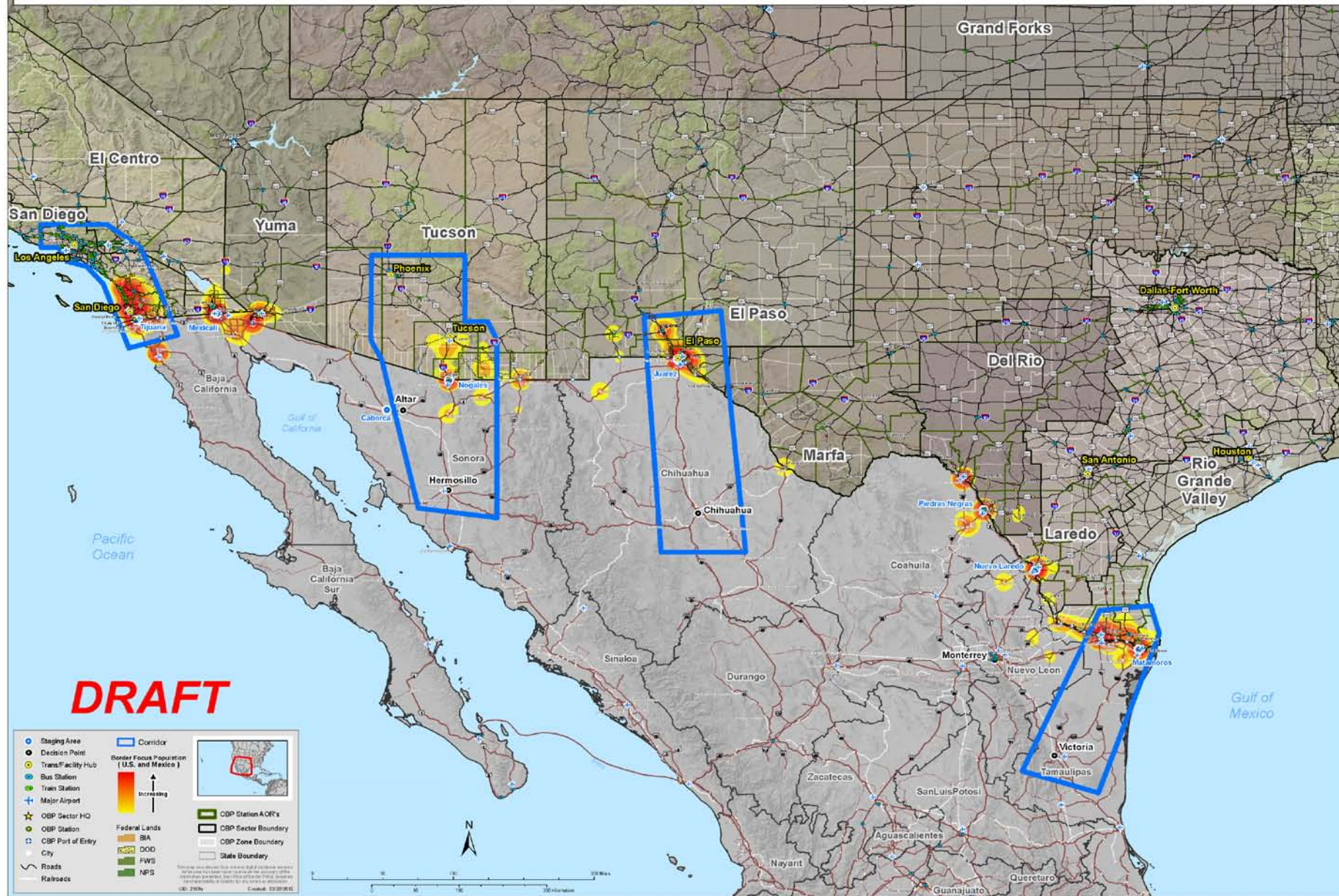
NOW - 2010

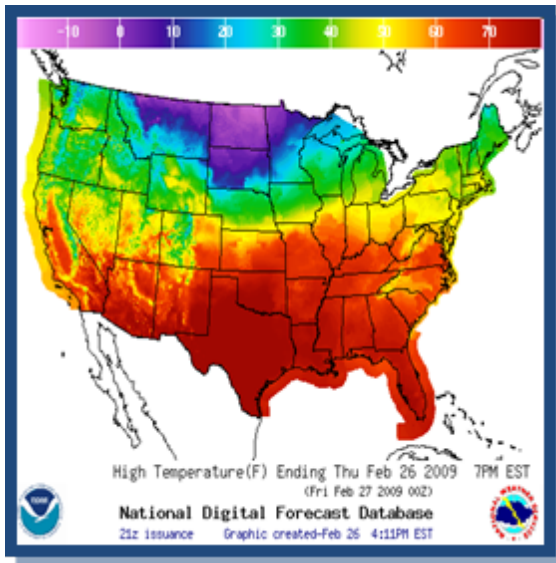
**81% Reduction in
Apprehensions**





Population Centers and Transportation Infrastructure Southwest Border





NOAA National Weather Service

Building a Weather-Ready Nation

Laura Furgione

NOAA Deputy Assistant Administrator
for Weather Services &

Deputy Director National Weather Service

Sept 28, 2010



Most Severe Weather on Earth

A Typical Year in the U.S.



**6 Atlantic
Hurricanes**



1,300 Tornadoes



5,000 Floods



**26,000 Severe
Thunderstorms**



**Drought and
Large Wildfires**



**600 Deaths
\$14B in Losses**

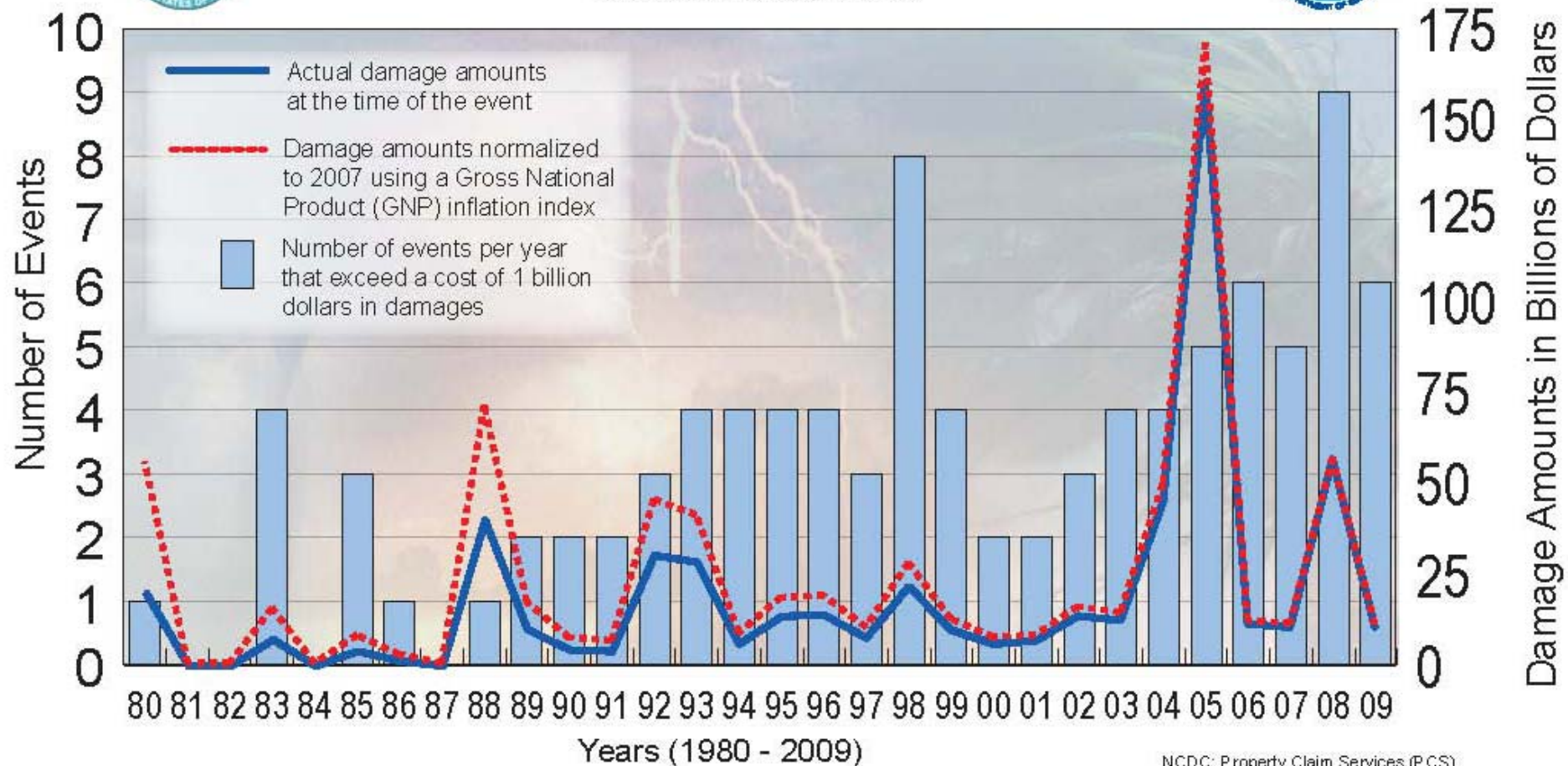
Most Severe Weather on Earth

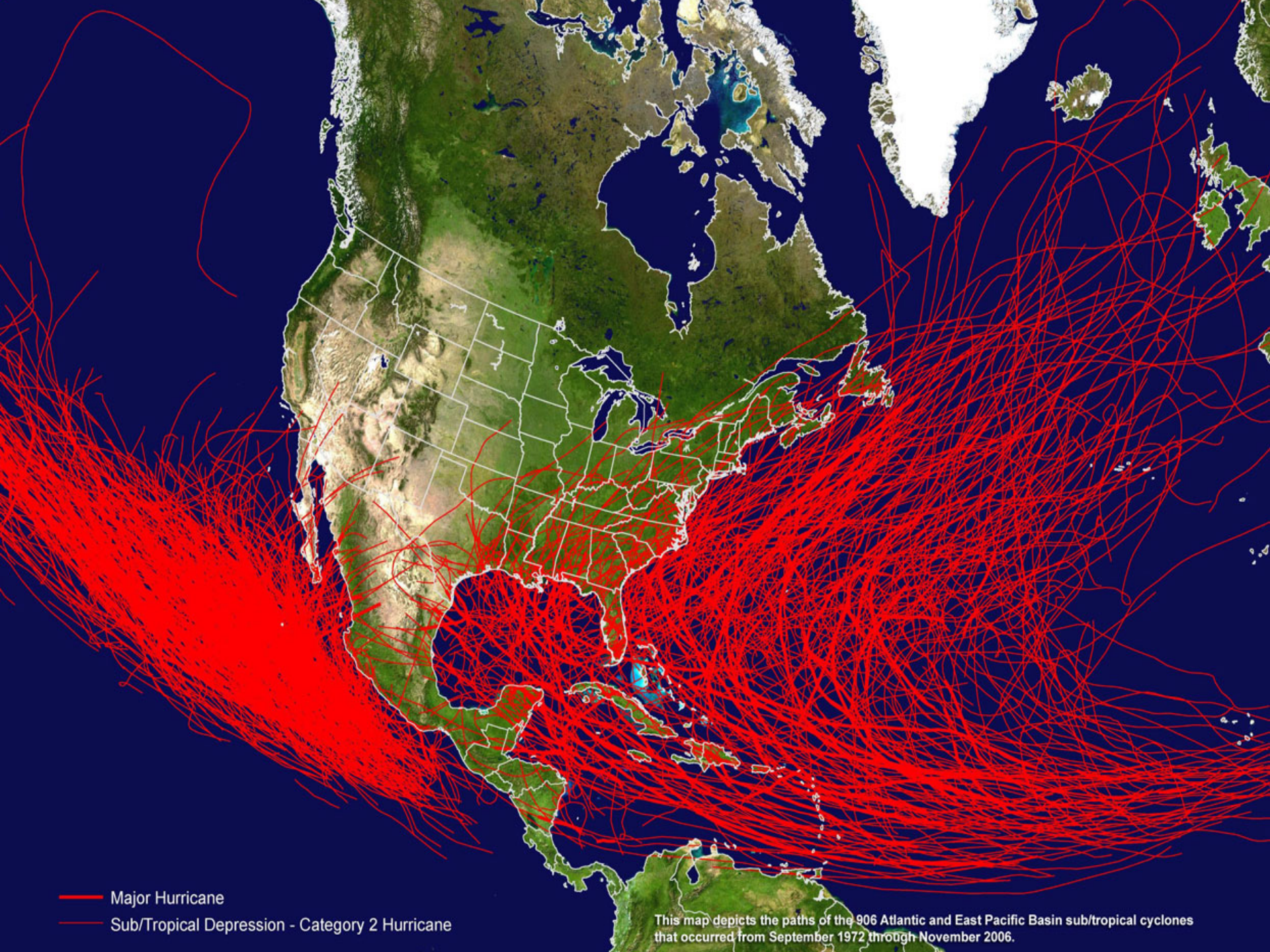
Billion Dollar Disasters



Billion Dollar U.S. Weather Disasters 1980 - 2009

NOAA/NESDIS/NCDC





- Major Hurricane
- Sub/Tropical Depression - Category 2 Hurricane

This map depicts the paths of the 906 Atlantic and East Pacific Basin sub/tropical cyclones that occurred from September 1972 through November 2006.



A Weather-Ready Nation

National Weather Service Strategic Plan 2020

SEARCH

☐ This Site
 ☒ All NWS

Explore the Plan
TOWARD A BETTER FUTURE

Achieving Our Vision
NWS GOALS

Weather Decision Services

Improve weather decision services for events that threaten safety, health, the environment, economic productivity, or homeland security

[Learn More >>](#)

THANK YOU FOR PARTICIPATING!

The public comment period has ended thank you for all of your constructive comments

Stay Connected
with IWS

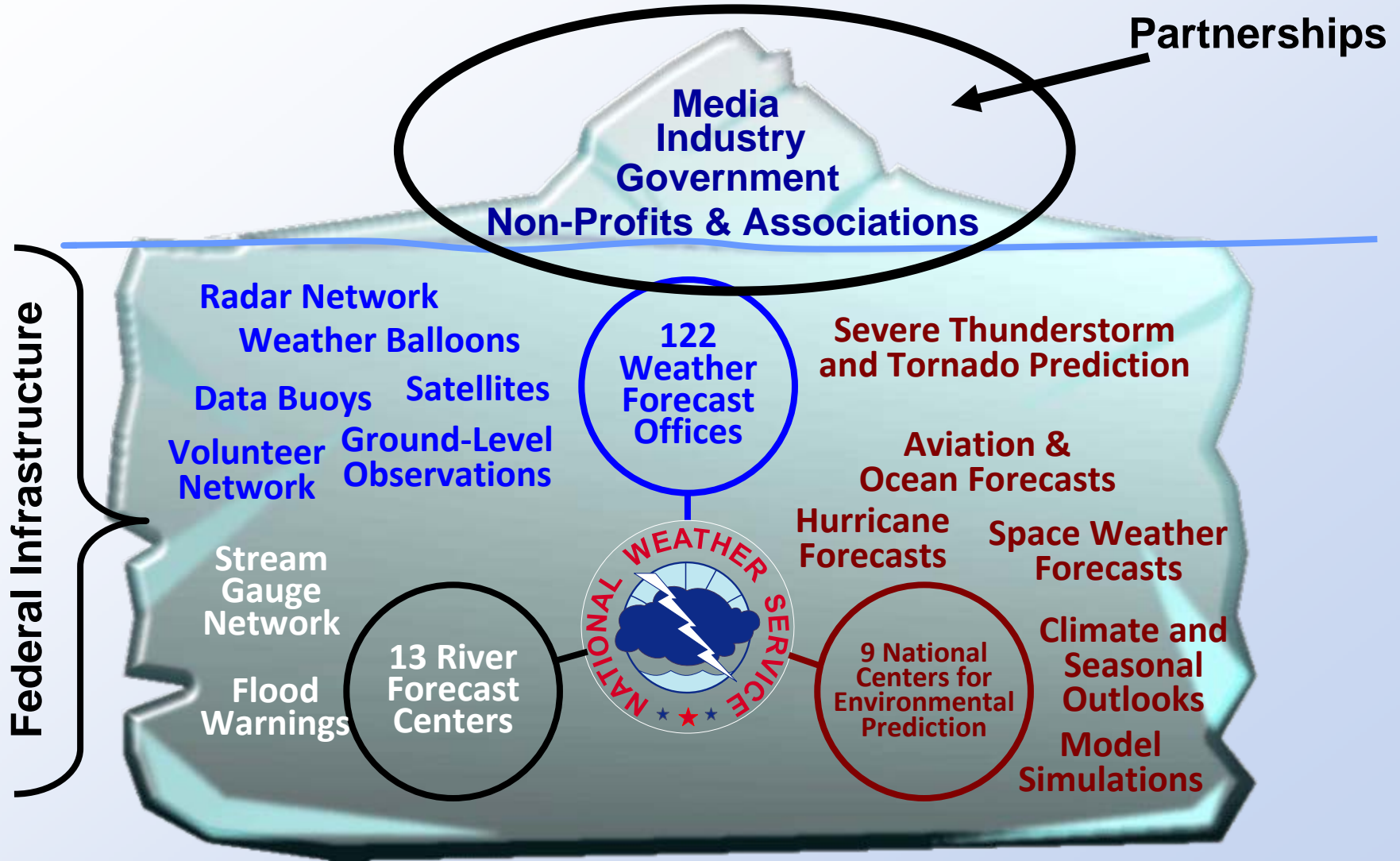


Message from Jack Hayes

NOAA Assistant Administrator for Weather Services and Director National Weather Service Jack Hayes introduces the NWS strategic plan and encourages everyone to participate in the feedback process

Building a Weather-Ready Nation

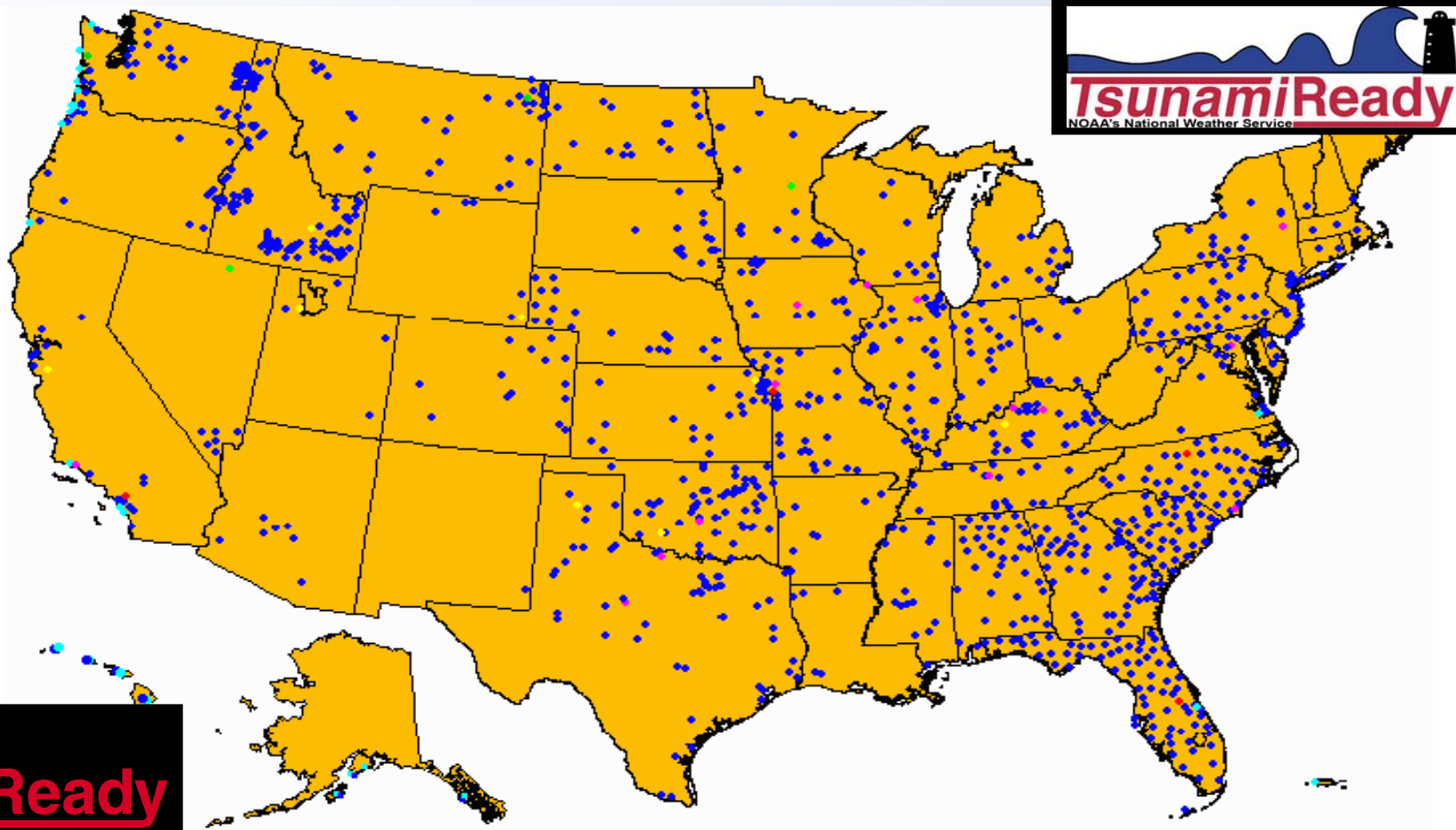
Partnerships are at the tip of the iceberg



Building a Weather-Ready Nation

Working at the Local Level

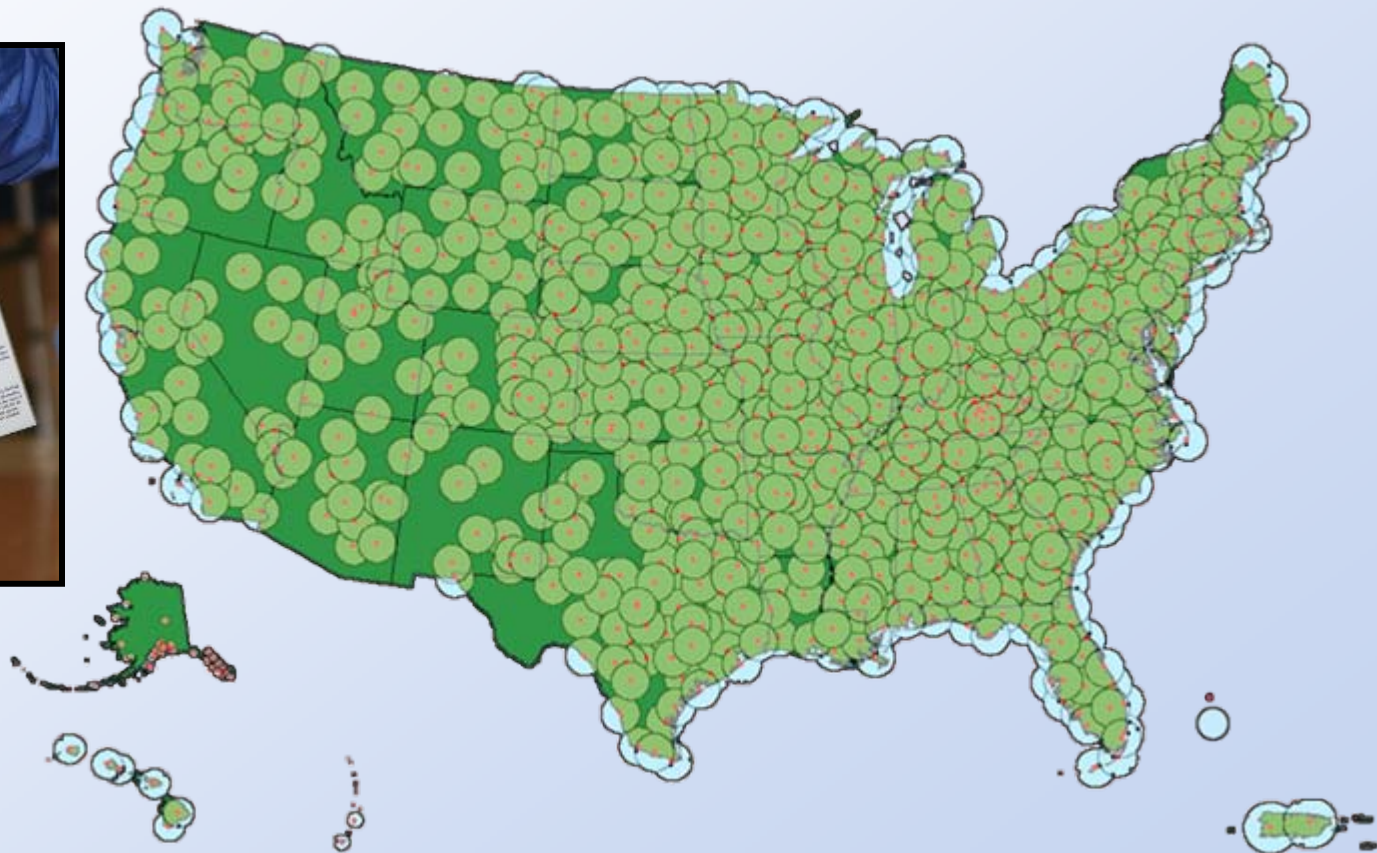
1,656 StormReady Communities in 50 States
79 TsunamiReady Communities in 10 States



Building a Weather-Ready Nation

NOAA Weather Radio—All Hazards

- ***1,000 transmitters***
- ***Available in All 50 States***



Building a Weather-Ready Nation

Tornado Warnings

January 10, 2008
Caledonia, MS

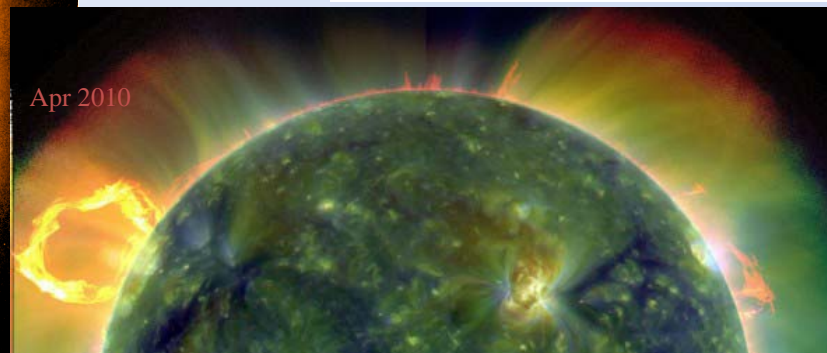
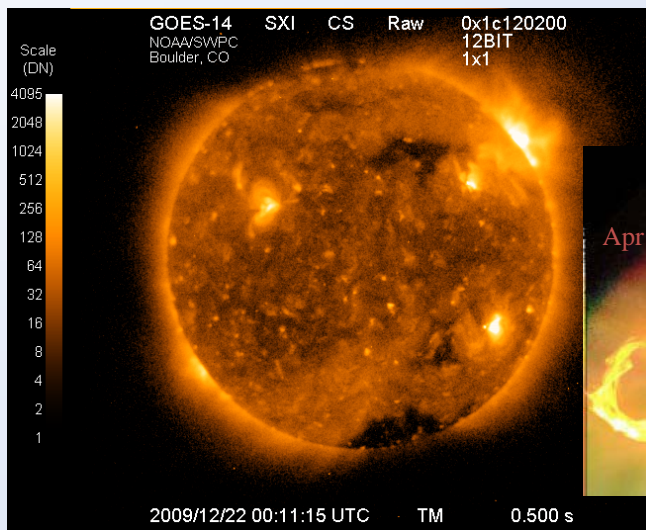
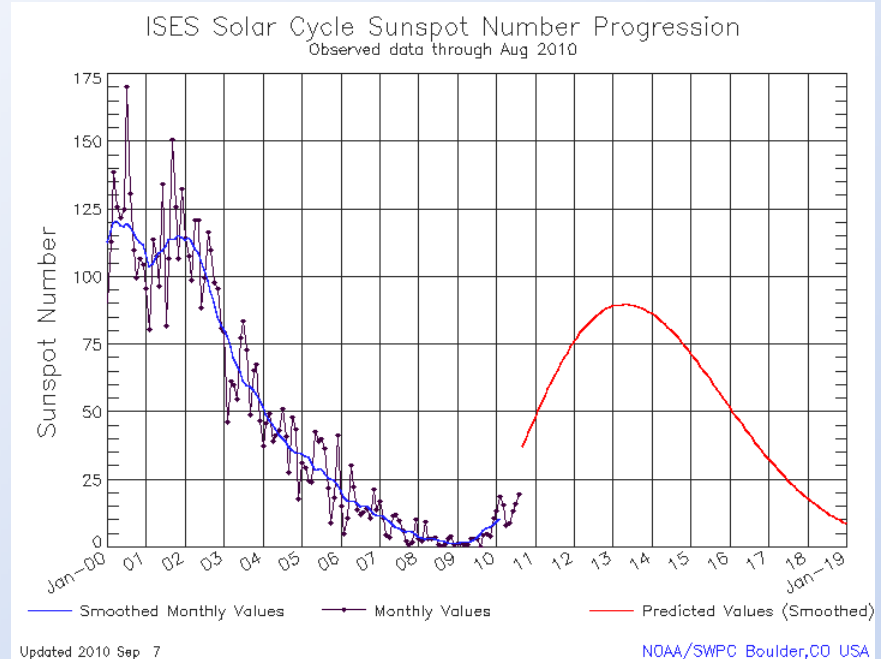


- EF-3 Tornado
- 41 minute lead time
- 2,000 people inside
no fatalities, 3 injuries

Building a Weather-Ready Nation

Space Weather

- Next solar maximum is expected 2013
- Space weather impacts:
 - Satellites (i.e. Galaxy 15)
 - GPS Reliability
 - Aviation (NextGen, Polar Flights)
 - Energy distribution
- \$1-2 Trillion potential impact



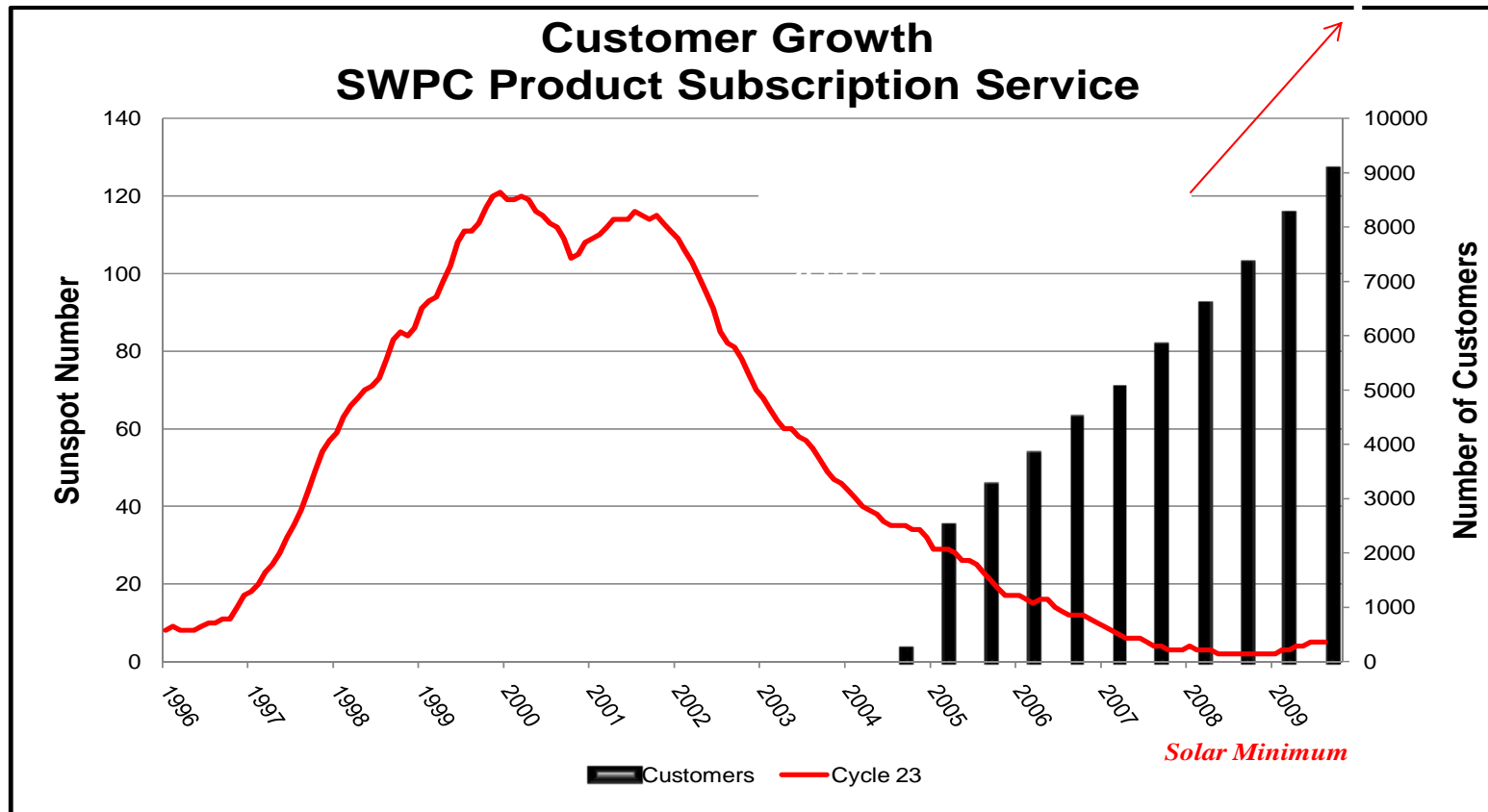
Space Weather Impacts

- On Oct 28, 2003 NWS space weather forecasters observed a powerful Earth-directed eruption on the Sun. Space weather warnings were issued. In response:
 - ***Power grid operators reduced system load, disconnected system components, and postponed maintenance.***
 - ***Airlines made critical decisions about route and/or altitude restrictions to flight operations.***
 - ***Satellite operators took action to mitigate impacts.***
 - ***Precision GPS users postponed operations or used back-up systems.***
- NWS working with FEMA and DHS to ensure critical infrastructures are safe from extreme space weather events.

<http://www.spaceweather.gov>



Protecting Our Advanced Technologies



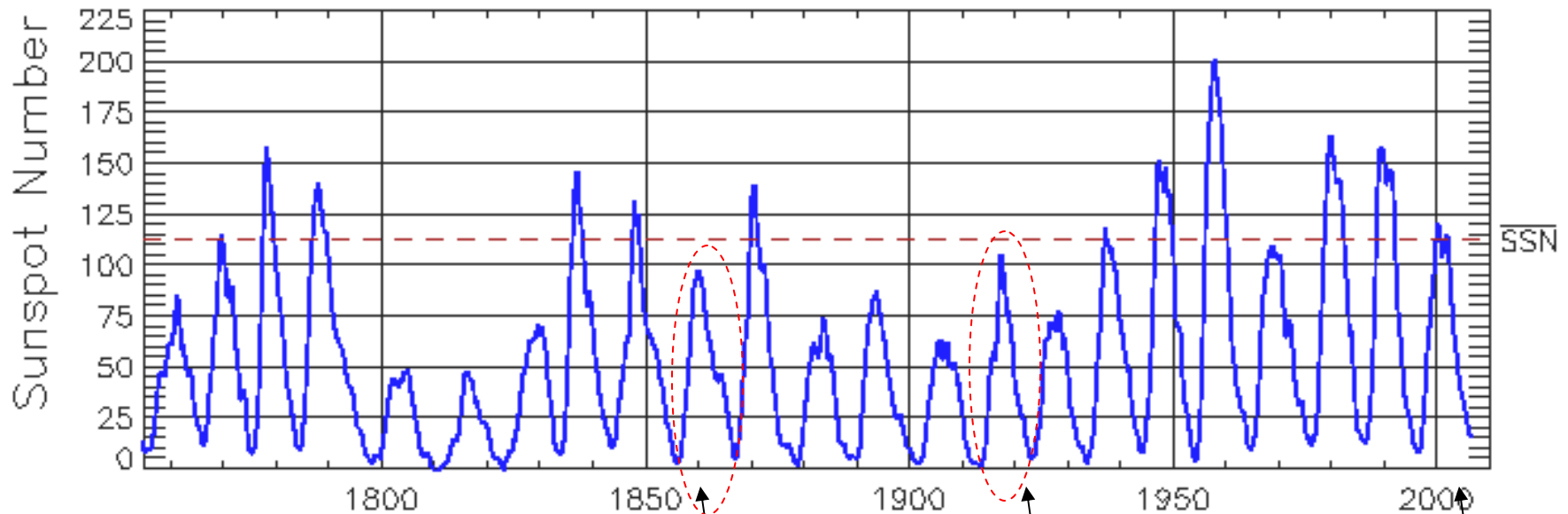
SES Satellite	Inmarsat	FEMA	Boeing	FAA
North America Electric Reliability Corp. (NERC)	L-3 Communications	Florida Division of Emergency Mgnt.	British Petroleum America	Bonneville Power Administration
Washington St. Dept of Transportation	Caterpillar, Inc.	Alaskan Airlines	United Launch Alliance	Salem and Hope Creek Nuclear Stations

Example of Registrants in 2009

Preparing for Extreme Space Weather

The largest geomagnetic storms on record occurred during lower than average cycles

The Solar Cycle in Sunspot Number



1859 Storm

1921 Storm

2003 Storm

Building a Weather-Ready Nation

Protecting Lives Through Partnerships

NOAA TEAM

PARTNERS

PUBLIC



FEMA

Building a Weather-Ready Nation

Working at the Local Level





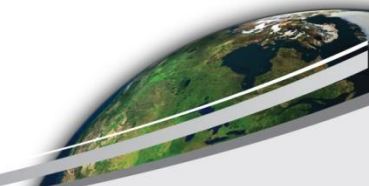


**2010 NDIA Homeland
Security Symposium**
September 28, 2010

VADM David Pekoske

9/22/2010 Testimony before the Senate Committee on Homeland Security and Government Affairs

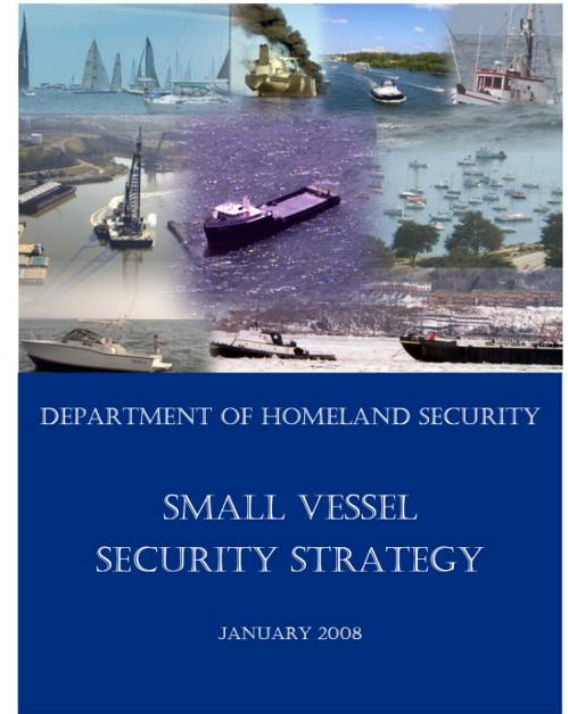
- **Homeland Security Secretary Janet Napolitano:**
 - “Homegrown terrorists represent a new and changing facet of the terrorist threat.”
 - “There is a rising threat from attacks that use improvised explosive devices (IEDs), other explosives and small arms.”
- **FBI Director Robert Mueller:**
 - “Despite significant counterterrorism pressure abroad, al Qaeda remains committed to advancing attack plans directed at the West, including plans against Europe and the homeland.”
- **NCTC Director Michael Leiter:**
 - “During the past year our nation has dealt with the most significant developments in the terrorist threat to the Homeland since 9/11.”



Small Vessel Security Strategy

Implementation Plan

- Pends DHS Approval
- IMO Guidelines
- Leg Proposal for Small Boat Operator Training and Certification
- AIS/NOA NPRM
 - Commercial > 65'
 - Tugs >26' or 600 HP
 - All vessels 50+ passengers
 - All high speed vessels
 - Barges carrying CDC



USS COLE (2000)
M/V Limburg (2002)
M/V Seabourne Spirit (2005)
Mumbai Attacks (2008)

Maritime Operational Threat Response



Ingredients:

- Triggers
- Coverage
- Responsiveness
- Decision Making
- Procedures

MAERSK ALABAMA

Utilized > 750 times
since 2006



Strategic Imperative: Move Borders Out

Offshore Capacity – CG's #1 Resource Need

Major Cutters began service in 1964 (46 YOA now)

High Endurance ('67-'72)

Medium Endurance

'64-'69

'83-'91



First two replacements were commissioned in 2008 and 2009; only 3 more funded so far

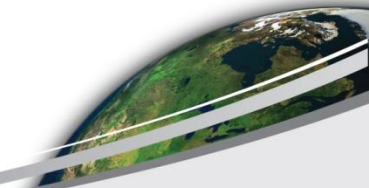
This is a very long term acquisition; projected to run for the next 20 years (2031)!

Integrity...

Commitment...

Quality Performance...

“Securing Your World”



DELIVERING CONFIDENCE

CSC

Government Keynote

Andy Purdy
Chief Cybersecurity
Strategist
CSC Cybersecurity

NDIA 2010 HOMELAND
SECURITY SYMPOSIUM &
EXHIBITION

September 29, 2010

CSC

Summary of Cyber Risk

- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.
- A spectrum of malicious actors routinely conducts attacks against the cyber infrastructure using increasingly sophisticated cyber attack tools.
- Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating effect.

Cyber News

- “Administration seeks ways to monitor Internet communications”
- “Big cybersecurity contractors turn to little firms for specialized monitoring services”
- “U.S. cybersecurity plans lagging, critics say”
- “Zeus botnets’ Achilles’ Heel makes infiltration easy”
- “Anti-piracy lawyers’ email database leaked after hack”
- “Cyber takes centre stage in Israel’s war strategy”
- “Iran confirms massive Stuxnet infection of industrial systems”
- “DOE Funds to Strengthen Grid Cybersecurity”
- “DoD Unveils New Cyber Defense Strategy --
Cyberspace Joins Land, Sea and Air as Fourth Arena of Warfare”

Good news in cyber

- Cyber Storm III
- National Cyber Incident Response Plan (NCIRP)
- White House Cyber Coordinator
- Cyber Command
- National Strategy for Secure Identities
- NIST/DHS – Risk Management and Continuous Monitoring
- DIB Program and IT Pilot
- New Cyber Funding
 - Electric grid security.
 - Innovative cyber solutions
 - Pilots
- Focus
 - Supply chain
 - Secure software
 - Situational awareness/incident response
 - Interoperability
 - Acquisition policy
 - Private sector input

Comprehensive National Cyber Initiative (CNCI)

- Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
- Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.
- Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Initiative #4: Coordinate and redirect research and development (R&D) efforts.
- Initiative #5. Connect current cyber ops centers to enhance situational awareness.
- Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
- Initiative #7. Increase the security of our classified networks.
- Initiative #8. Expand cyber education.
- Initiative #9. Define and develop enduring “leap-ahead” technology, strategies, and programs.
- Initiative #10. Define and develop enduring deterrence strategies and programs.
- Initiative #11. Develop a multi-pronged approach for global supply chain risk management.
- Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

Why is the DIB Initiative Important?

- The DIB Cyber Security Program is a major effort to support National Security – It is one of 18 Critical Infrastructures.
- Provides access to threat information and data to proactively implement safeguards throughout the enterprise
 - Information obtained through the DIB will enable providers to more securely support clients in the DoD and Critical Infrastructure
- Strengthens existing Information Risk Management Programs
- Membership in the DIB will highlight the security/trustworthiness of quality providers' services and solutions
- The DIB Pilot requirements are expected to become Federal Acquisition Requirements over the next year

Cyber Attacks Against Critical Infrastructure

Driver for Cybersecurity Services -- Vulnerability of Industrial Control Systems

- The Stuxnet worm, reportedly the most sophisticated malware ever, has targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility companies since at least Jan 2010.
- Speculation that Stuxnet was created by a state-sponsored team of programmers, and designed to cripple Iran's Bushehr nuclear reactor.
- Infected at least 30,000 Windows PCs in Iran; Iran's Atomic Energy Organization reportedly met recently to discuss how to remove the malware.
- Microsoft acknowledged that the worm targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility companies.
- Those control systems, called SCADA, for "supervisory control and data acquisition," operate everything from power plants and factory machinery to oil pipelines and military installations.

Source:

http://www.computerworld.com/s/article/9188018/Iran_confirms_massive_Stuxnet_infection_of_industrial_systems

“Call it what you will...an international struggle in cyberspace...economic, political, military”

For to win one hundred victories in one hundred battles is not the acme of skill.
To subdue the enemy without fighting is the acme of skill.

Sun Tzu

A Three Stage Escalation...we are engaged in Stage 2

Stage 1: Passive Exploitation

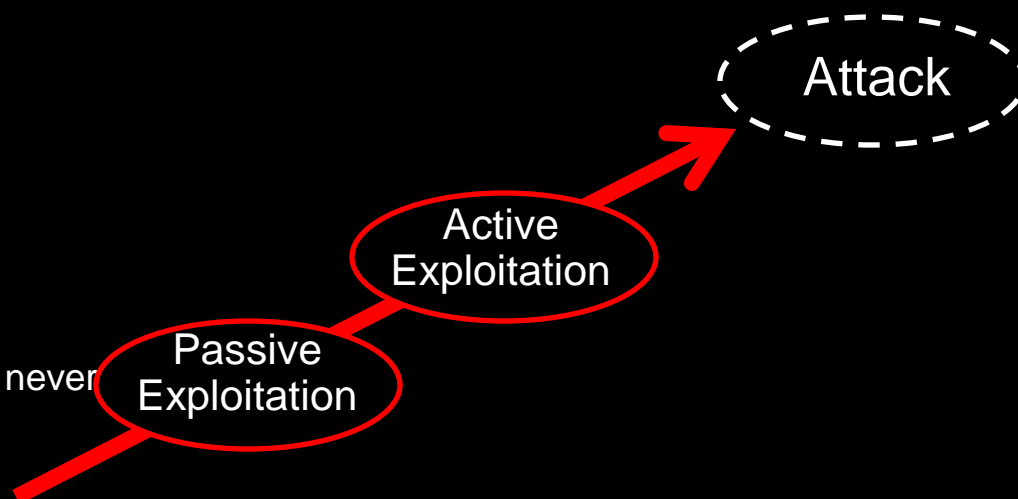
- Reconnaissance
- Mapping, Code Injection
- Find weaknesses

Stage 2: Active Exploitation

- Steal blueprints
- Create Disinformation
- Success would mean that there may never be a need to go to Attack

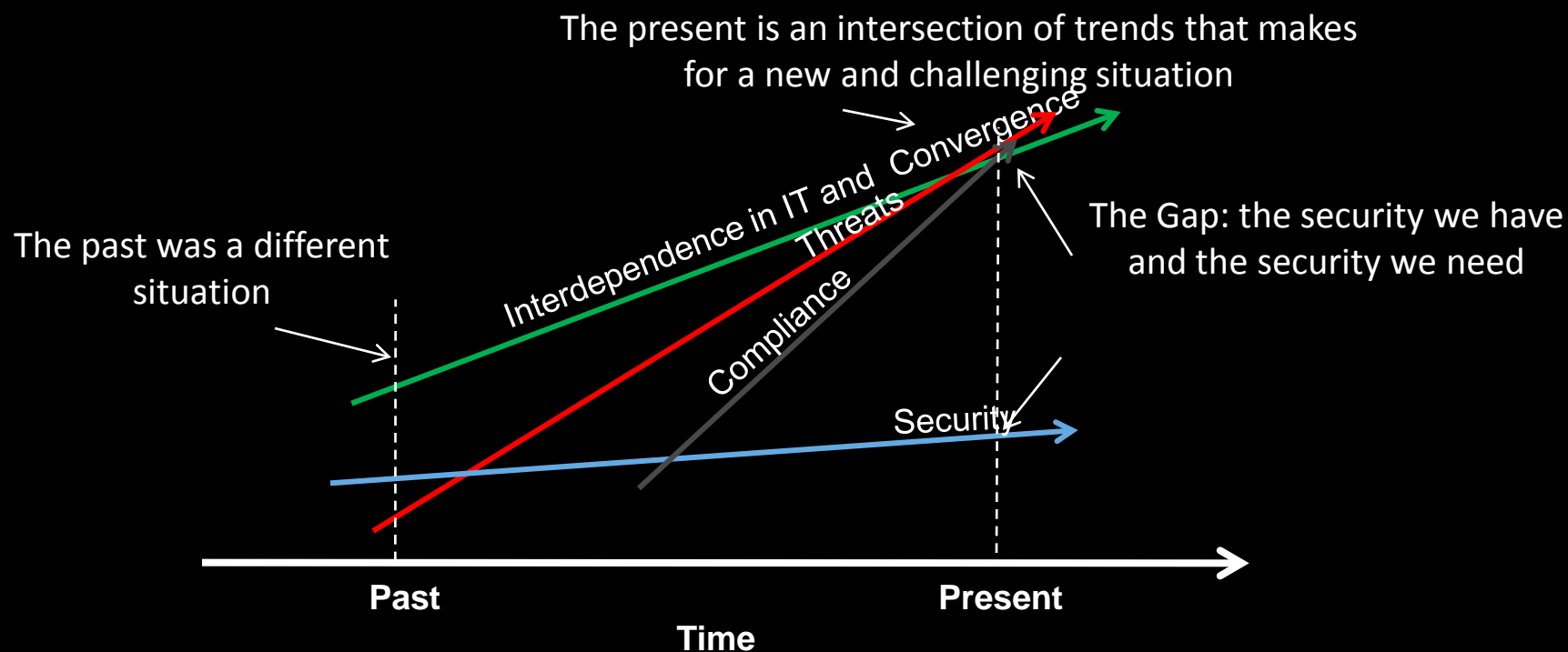
Stage 3: Attack

- Take down a utility
- Disrupt a supply chain
- Create financial mis-trust



*“It’s asymmetric because...
those intent on harm: are everywhere, may not be an
organization at all, unconstrained by geo-political
boundaries, can’t pin attribution with certainty, motives
are boundless, and groups combine not unlike business
partners in a commercial market”*

What's different between then and now...



It may be that the question is not of ROI – but do you want to stay in business – a corporate and a national question

Lessons we should understand...

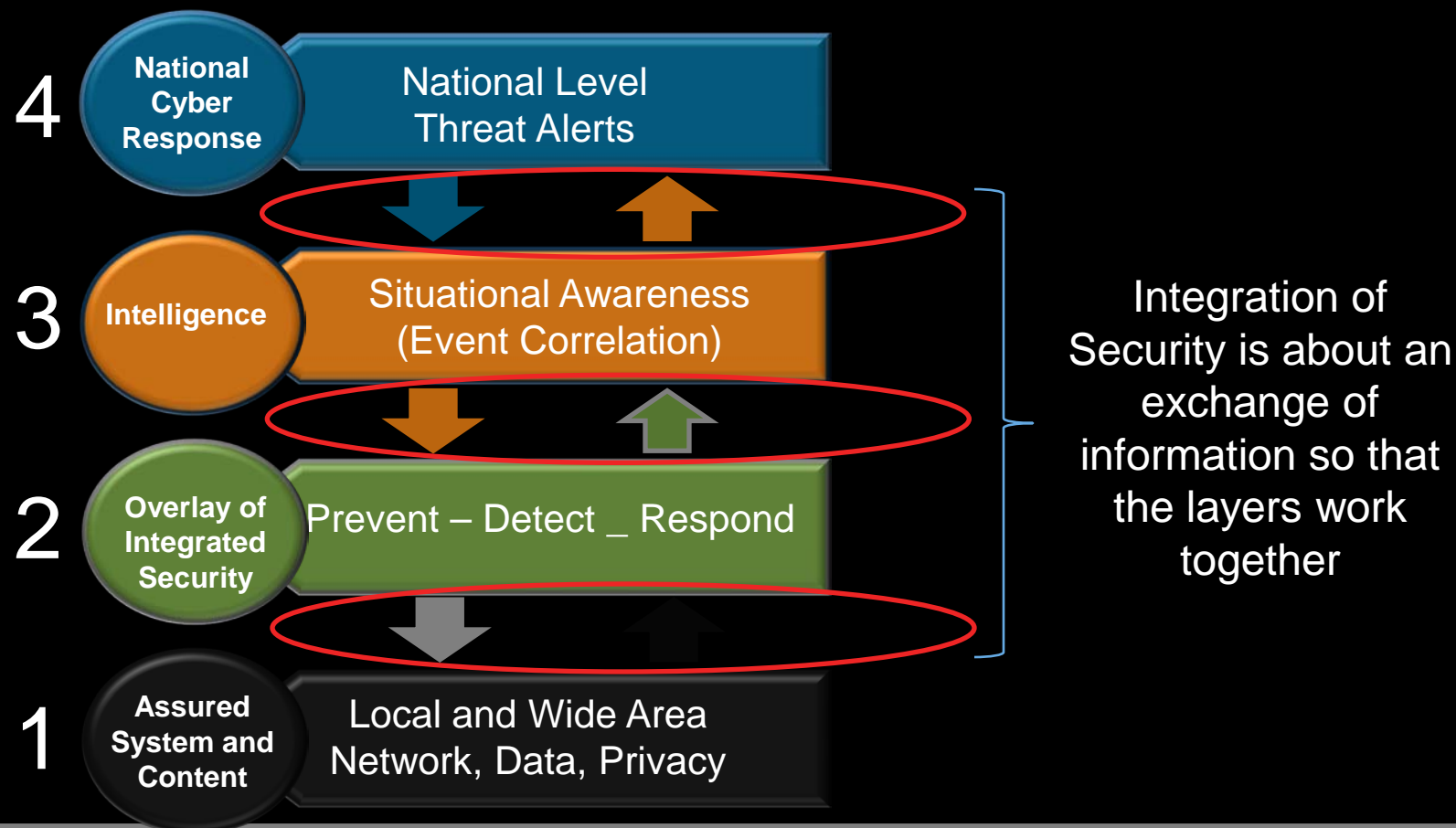


- Witnessing the depletion -- loss of competitive advantage
- It's a new world – new generation of threats
- Adversaries are in our systems
- Compliance (penalties) more stringent – not less
- Answers: Security must be designed in (architected)
- Bolt-on security insufficient to the present task
- Stage 2 (Active Exploit) is here to stay
- You will not hear a bang – maybe a hiss (air escaping); maybe nothing
- Time to wake up to this reality

“The Security Stack”

Designing Security In: “The Security Stack”

Measuring up - to a new generation of threats

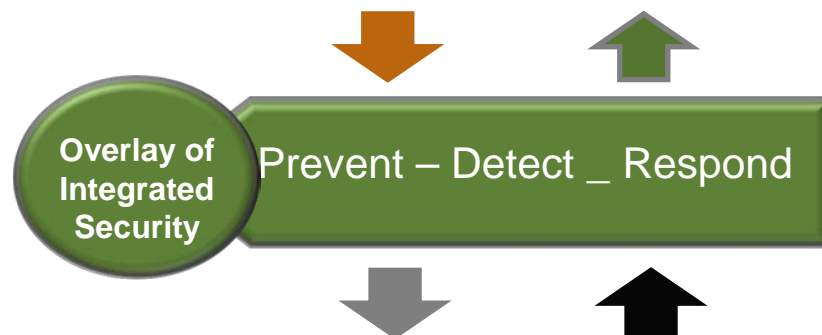


The Cybersecurity Stack (Layer 1)



- Architecting (designing-in) the security
 - Enclave Isolation
 - Configuration Management Data Base
 - Endpoint Protection
- Privacy Requirements
 - Data Classification
 - Encryption
- Takes security solution engineers
 - Working with our solution architects
- Requires integration with Layer 2 functions
 - Unauthorized Configuration Information passed up to L2

The Cybersecurity Stack (Layer 2)



- Integrating the security overlay
 - Firewalls
 - Security Manager
 - Intrusion Detection – Prevention
 - Data Loss
- Takes security solution engineers
 - Working with our solution architects
- Requires integration with Layers 1&3 functions
 - Example: Unauthorized Configuration Information passed up to L2

The Cybersecurity Stack (Layer 3)



- Integrating situational awareness
 - Event Correlation
 - Incident Management
 - Threat Indices - External
- Takes security solution engineers
 - Working with our solution architects
- Requires integration with Layers 2&4 functions
 - Example: Log information looking at trends, multi-threaded attacks, signatures, integration with external sources of threats (indices)

The Cybersecurity Stack (Layer 4)



- Integrating situational awareness with Government – for critical infrastructure companies
 - Threat Indices – External
- Requires integration with Layer 3 functions
 - Example: government provided threat indices

A Strategic View of ICT Security

- There is no real separation in cyberspace; we share a common environment with allies, partners, adversaries, and competitors.
- It is important to understand computer network defense, and be informed by exploitation and attack.
- Security is more about architecture and integration than about deployment of more products to build perimeter defenses.

Public Sector aggressively investing in Cyber Solutions driven by increase in severity and number of attacks.

The U.S. public sector has seen an increased investment in cyber security technologies and has begun to coordinate cybersecurity activities, set cyber security R&D goals and create frameworks for public/private partnerships.

Drivers

- Exponential increase of data flows over government networks.
- U.S. adversaries perceive our dependence on information technology and our cybersecurity weakness as exploitable.
- Increased endpoint security risks from mobilized workforce.
- Confidential information leaks via Web 2.0 applications.
- Increase number of data breach incidents.
- Increased use of virtualization technologies such as cloud computing and open source applications.

Public/Private Partnerships

- Aligning of national defense with critical infrastructure.
- Private sector designs & operates public sector infrastructure.
- Public sector must defend infrastructure.
- Private sector reluctant to share information due to threats against their intellectual property due to Freedom of Information Act.
- Industry also needs the government to protect their competitive, proprietary data for economic advantage.

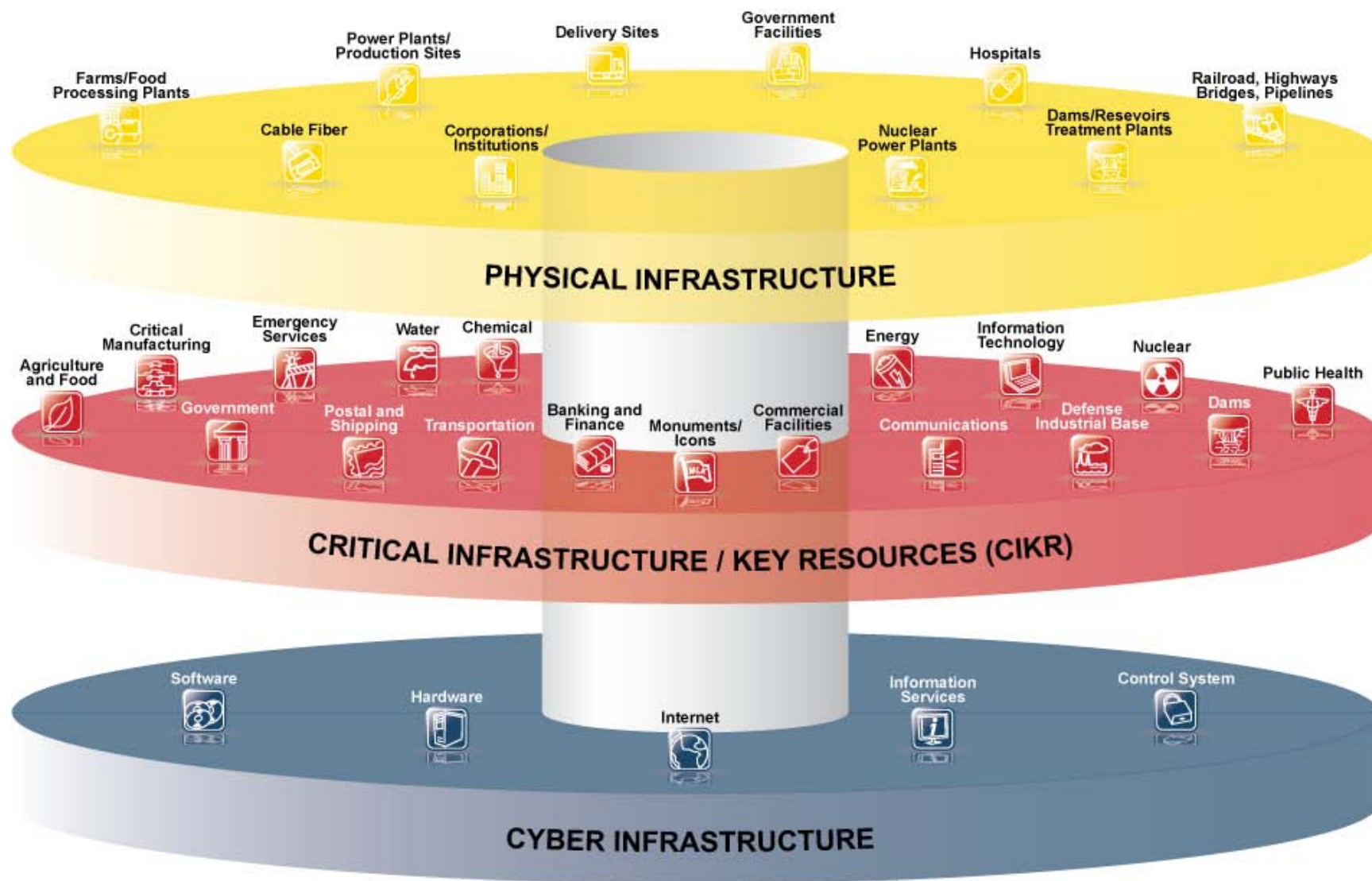
Cybersecurity – a National Security Imperative and Global Business Issue

- Nations and critical infrastructure owners and operators are dependent on Cyber for national security, economic well-being, public safety and law enforcement, and privacy.
- Major companies must ensure the resiliency of their operations, protect their reputations and the privacy of their customers, differentiate their brand, and meet compliance obligations.
- Innovative technologies and information assurance strategies must be implemented by government and private companies through fully integrated, end-to-end cyber solutions

Public Policy Challenge

- Nations are dependent on cyber for national security, economic well-being, public safety, and law enforcement
- Risk is real but not visible and obvious
- Authority/control is spread among multiple entities in the public and private sectors
- ICT is international
- Individuals and organizations are reactive and tactical, not proactive and strategic
- We do not learn lessons from the past

Cyber infrastructure underpins critical elements of CIKR



What is needed nationally and internationally?

A strategic approach to facilitate public/private collaboration and information sharing to set requirements, and resource, execute, and track progress on national strategic priorities:

- ICT risk;
- ICT preparedness;
- Malicious activity and cyber crime; and
- Research and development.

How should the challenge of ICT risk and preparedness be addressed?

- Stakeholders at the organizational, national ,and int'l levels must work together
 - to identify critical functions,
 - assess and mitigate risk, and
 - plan, and build capacity for, response and recovery
- Use standards to drive risk reduction
- Exercise to identify gaps and improve
- Pursue innovation
- Use this process to identify requirements to drive resource allocation for risk mitigation, response preparedness, and research and development

What do we need to do? How are we doing?

1. Private sector needs a seat at the table of decision-making.
 - Need representatives to the IPC and IPC sub-working groups.
2. Identify strategic priorities for public/private collaboration informed by input from private sector and government representatives:
 - Cyber risk;
 - Cyber preparedness;
 - Malicious activity and cyber crime; and
 - Research and development.
3. Each priority requires goals, objectives, and corresponding metrics and milestones.
 - Helps in setting resource requirements.
 - Promotes accountability by government (Executive and Legislature) and by private sector.
 - Makes it possible to track progress and inform areas of improvement.
4. International agenda should further strategic cyber priorities

Cyber Risk

- Nation's threat paradigm needs to be replaced by a risk paradigm (threat, vulnerabilities, and consequences);
- We need a national cyber risk assessment that spells out what the nation needs to worry about and what we need to do about it;
- Using a risk focus, expand the NIE (threat) model of broad-based government participation, to include private sector.

Cyber Preparedness

- Set requirements for situational awareness and a common operating picture for government and critical infrastructure
- Set requirements for a a public-private collaborative framework to address cyber incidents:
 - Analysis
 - Response
 - Recovery

Research and Development

- The nation must develop a national cyber R&D agenda to better assess and mitigate risk, enhance preparedness, and address the long-term hard problems we face in cyberspace
- The agenda must be informed by government and private sector, academia, and our closest allies.

Malicious Activity

- We must act strategically and proactively
- Malicious activity is a key component of ICT risk -- one part of a continuum of risk that the nation faces from terrorists, sophisticated hackers and hacktivists, organized criminal groups, and nation states (and those working for them).
- Law enforcement must work across government and with the private sector to prioritize action and resources, track progress, and impact malicious activity to reduce risk.
- Accountability is key to progress.

Malicious Activity/Cyber Crime

- U.S. must work nationally and internationally to address the underlying problem that there are virtually no consequences for malicious activity in cyberspace.
- Government and private sector should partner to collect and share data on the most significant malicious actors & enablers
- Coordinate efforts to shut them down and reduce frequency, impact, and risk of malicious cyber activity
- Mitigate the circumstances and vulnerabilities that allow them to operate
- Encourage private lawsuits as a complement to law enforcement

Protecting Your Organization, Clients, and Customers

- Improve your enterprise using:
 - an architectural approach,
 - assess it against appropriate standards,
 - implement a risk management program including continuous monitoring technology, and
 - subject your enterprise to periodic, independent assessments.
- Use lessons learned from Advanced Persistent Threats (APTs) and other sophisticated attackers to strengthen active defense
- If possible, join the Defense Industrial Base Pilot Program
- Work in public-private partnerships (e.g., ISACs, Sector Coordinating Councils, InfraGard, Electronic Crimes Task Force, National Cyber Forensics and Training Alliance, and associations) to strategically collaborate and share information about threat and risk

Andy Purdy
dpurdy@csc.com



BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

<http://www.csc.com/cybersecurity>

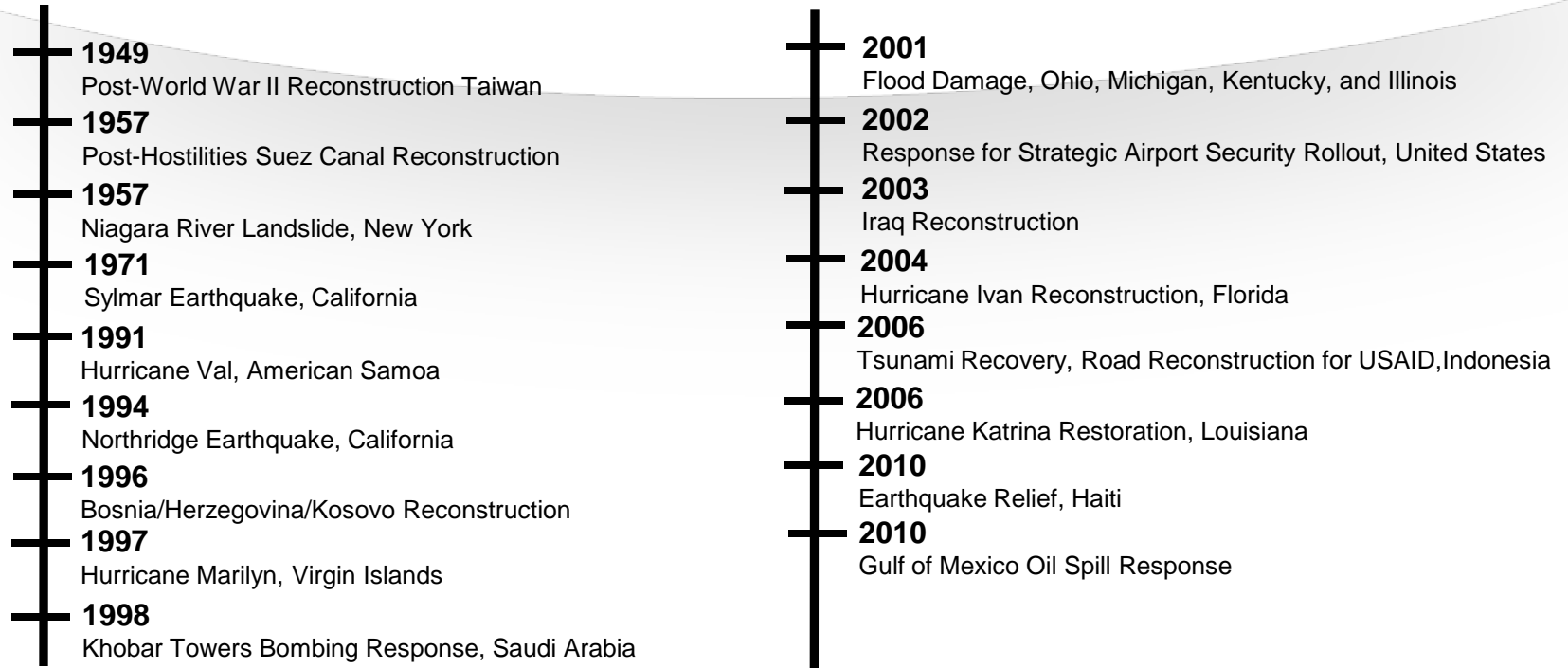
Parsons Industry Perspective On Consequence Management

NDIA Homeland Security National Symposium:
Panel: Wrath and Consequences of "Mother Nature"
September 28, 2010



Parsons History of Disaster Response

PARSONS

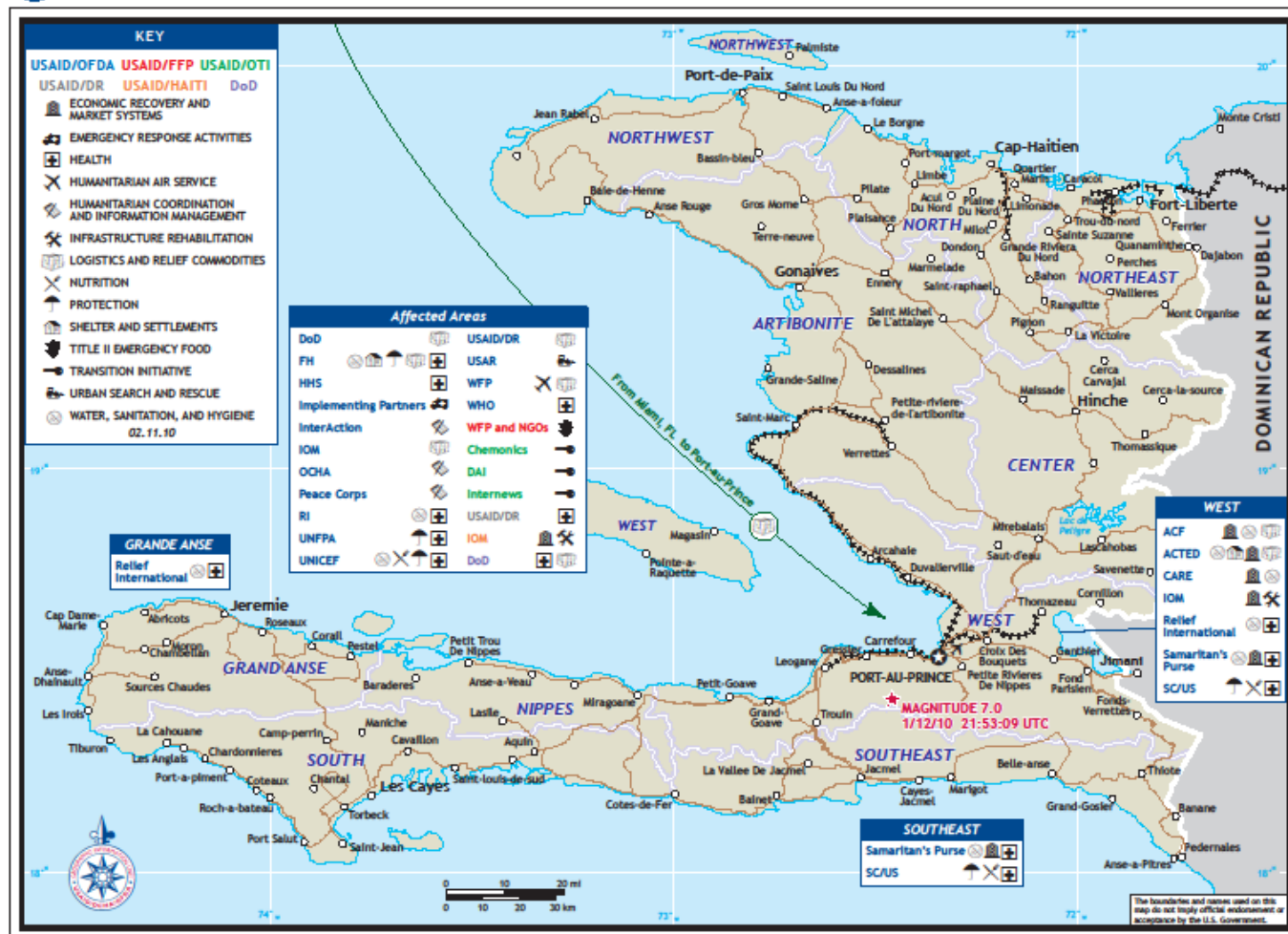


1-12 Haiti

PARSONS



USG HUMANITARIAN ASSISTANCE TO HAITI FOR THE EARTHQUAKE



1-12 Haiti

PARSONS



1-12 Haiti Parsons Activities

PARSONS

- Response
 - Naval Facilities Engineering Command
- Recover/Reconstruct
 - US Agency for International Development

NPS/1-12 similar effects

PARSONS

- Event
 - Major Earthquake
 - Major Hurricane
- Government Capabilities
 - Improvised Nuclear Device
 - Cyber Attack
 - Improvised Explosive Device
- Respond: Medical Countermeasures
 - Blister Agent
 - Nerve Agent
 - Aerosol Anthrax
 - Pandemic Influenza
 - Plague

NPS/1-12 similar effects

PARSONS

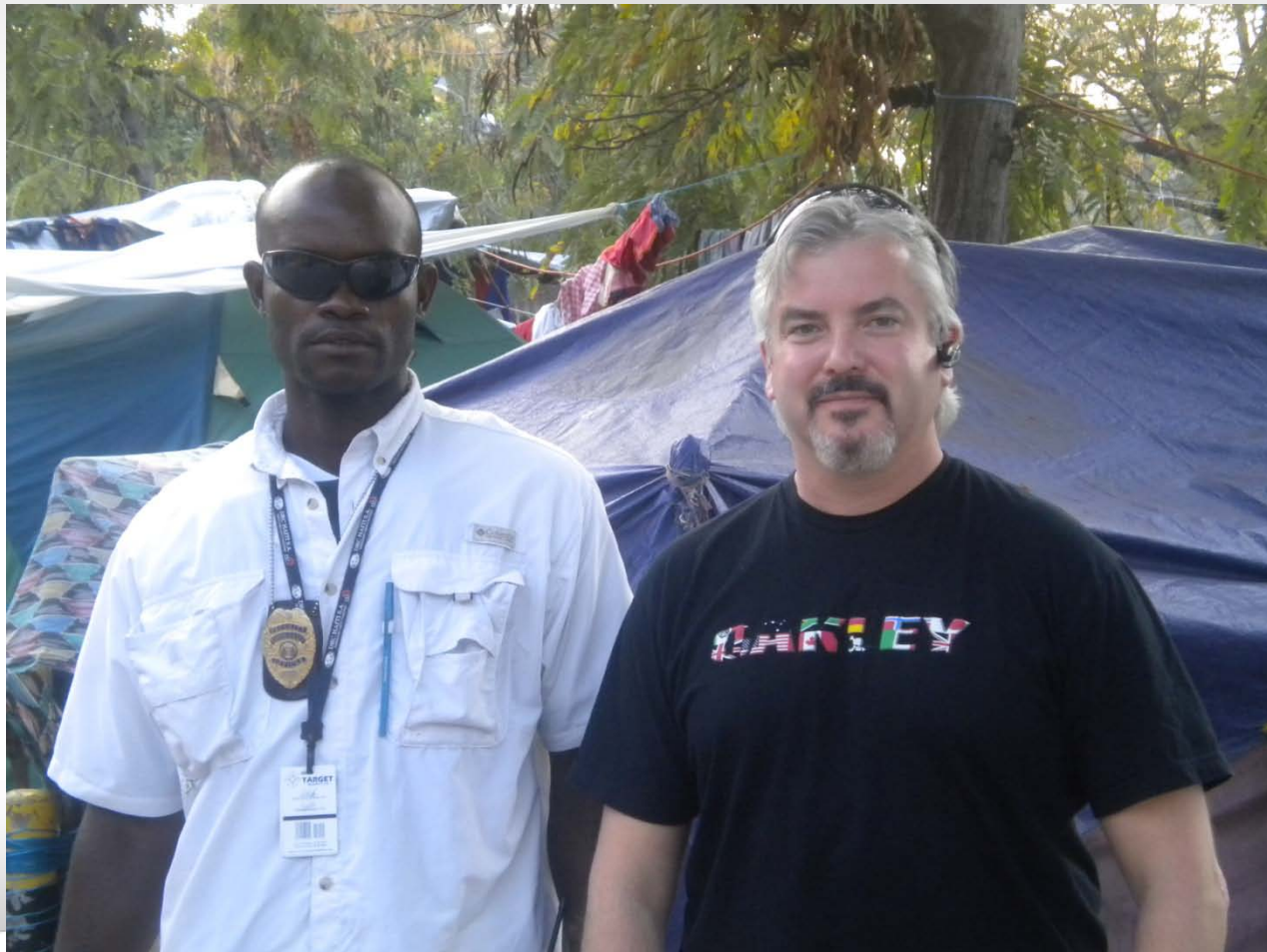
- Respond: Decontaminate
 - Toxic Industrial Chemicals
 - Chlorine Tank Explosion
 - Radiological Dispersal Device
- Recover and Reconstruct
 - Food Contamination
 - Foreign Animal Disease



A dynamic disaster environment

PARSONS

Got Security?



More Public/Private Up-Front Interaction

PARSONS

Before Disaster Strikes

Imperatives for Enhancing
Defense Support of Civil Authorities



The Report of the
Advisory Panel on Department of Defense Capabilities for Support of Civil Authorities After Certain Incidents
to the Secretary of Defense and the
Chairmen and Ranking Minority Members,
Committees on Armed Services,
U.S. Senate and U.S. House of Representatives

September 15, 2010

“Recommendation: That the President direct the establishment of an integrated planning system that promotes coordinated planning among local, State, and Federal Government entities and the private sector and that includes provisions for support from international organizations and friendly and allied governments, especially Canada and Mexico.”

Improving Regional Resilience: Bringing It All Together

Yazmin Seda-Sanabria

Senior Program Manager

Critical Infrastructure Protection & Resilience Program

U.S. Army Corps of Engineers, Headquarters

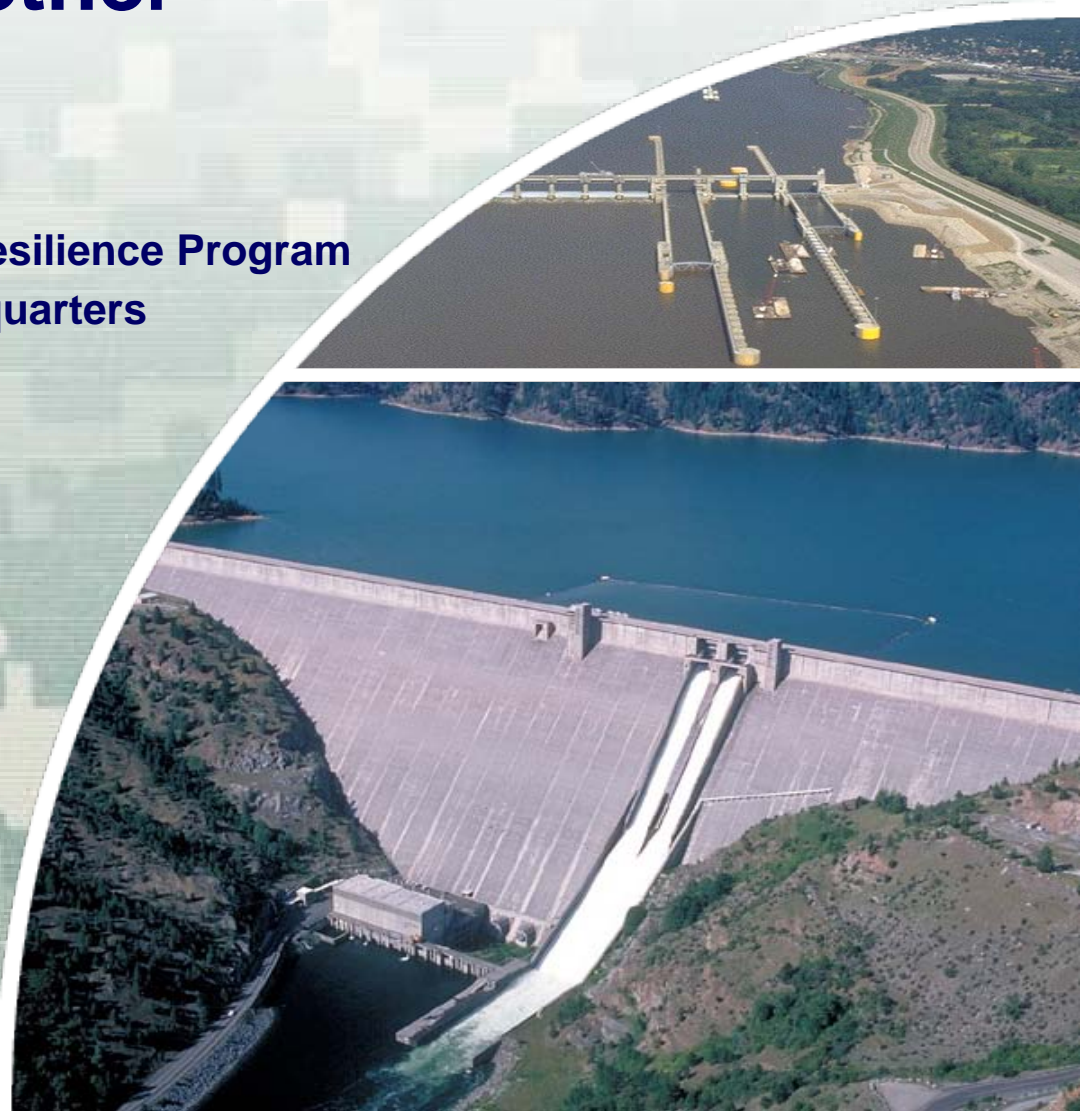
2010 NDIA Homeland Security Symposium

28-29 September 2010

Arlington, Virginia



US Army Corps of Engineers
BUILDING STRONG®



Dams as Critical Infrastructure

- Dams Sector encompasses not only “conventional” dams but also locks (and navigation dams), levees (flood protection systems), hydropower facilities, mine tailings, and other water retention or control structures.
- DHS Office of Infrastructure Protection designated as Sector-Specific Agency.



Dams...



Locks...



... and Levees



U.S. Army Corps of Engineers (USACE) as Dams Sector Stakeholder

627 Shallow Draft Harbors

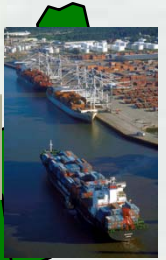


25% of Nation's
Hydropower
Production



383 Major Lakes
&
Reservoirs
376 M visitors/yr

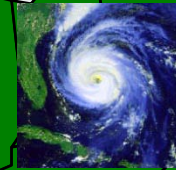
299 Deep Draft Harbors



400 miles
Coastal
Structures



11,000 miles
Inland
Waterways



Emergency
Operations

4340
Recreation
Areas



653 Dams
276 Locks

14,000 miles of
Levees



\$500M annual
Dredging Costs



11.7 Million Acres
Public Lands



Environmental
Stewardship



Regulatory
Responsibilities

Cumulative Flood Damage Reduction >\$419 Billion

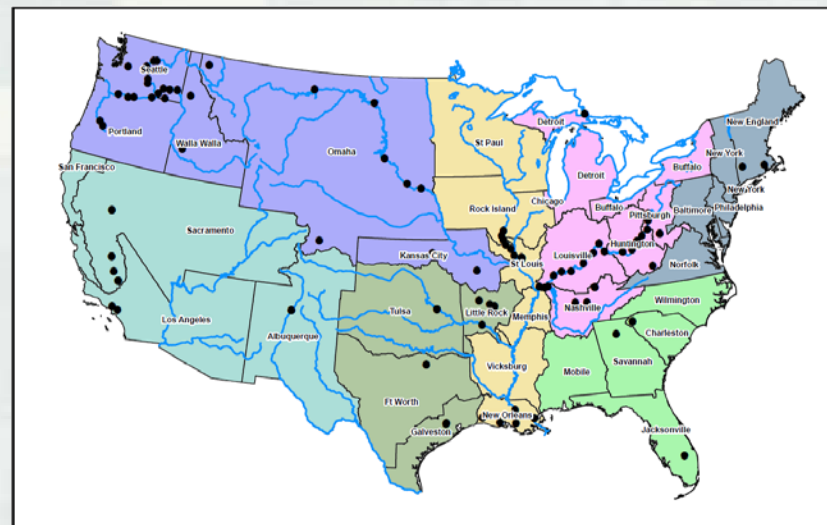
USACE Critical Infrastructure Protection & Resilience (CIPR) Program

- **Program Goal:**

- Improve protection, resilience, and lifecycle investment in critical infrastructure.

- **Program Vision:**

- Achieve a more secure and more resilient civil works critical infrastructure by enhancing its protection in order to prevent, deter, or mitigate the effects of manmade incidents and improve preparedness, response, and rapid recovery in the event of an attack, natural disaster, and other emergencies.



- **Integrated Approach:**

- Portfolio-Centric
- System/Regional Focus
- All Hazards Coordination

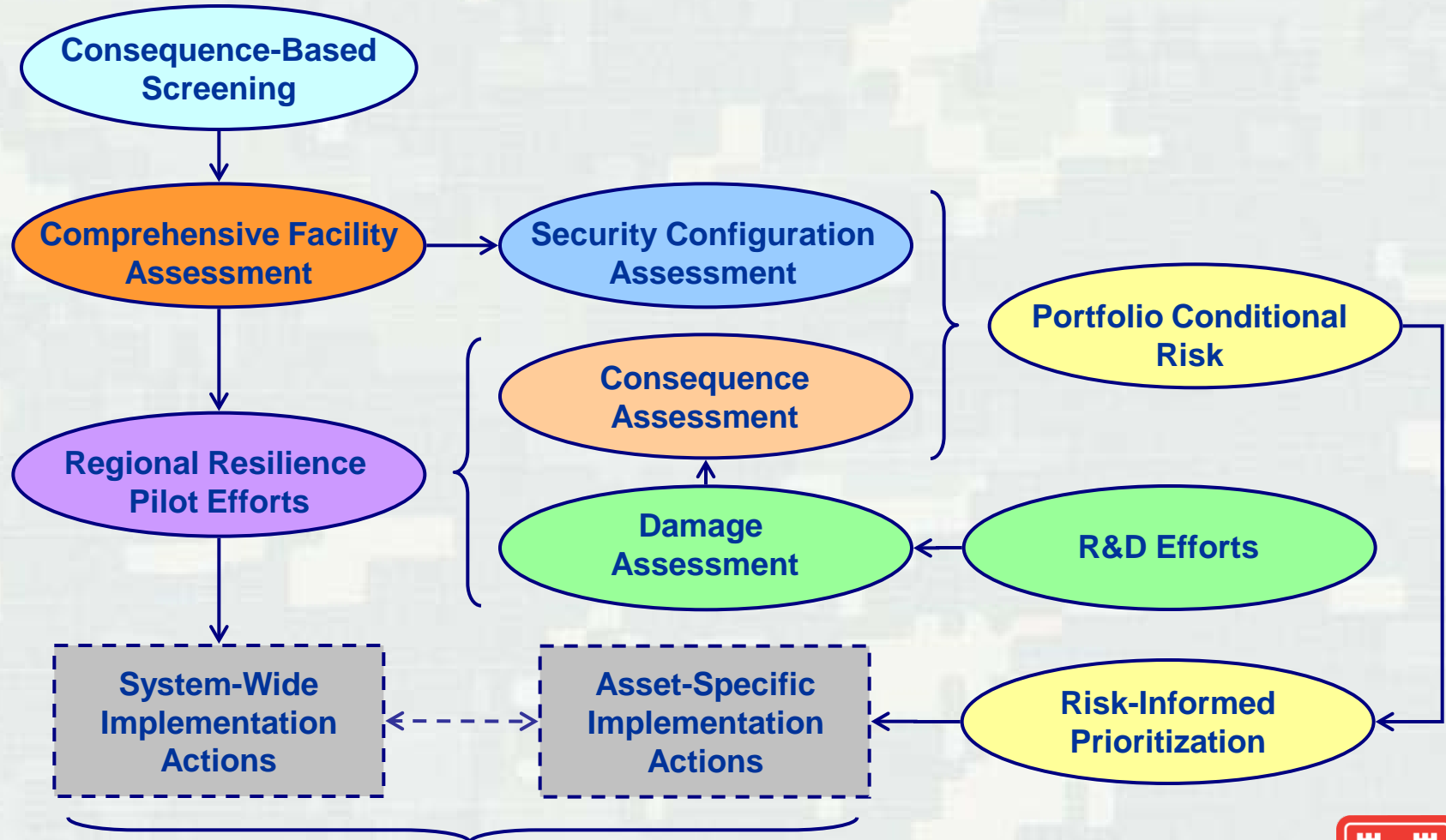


Challenge: A Complex Risk Profile

- **Driven by multiple sources:**
 - **Natural hazards**
 - **Structural deficiencies**
 - **Aging**
 - **Accidents**
 - **Malfunctions**
 - **Deliberate aggressor actions**



USACE Critical Infrastructure Protection & Resilience (CIPR) Program

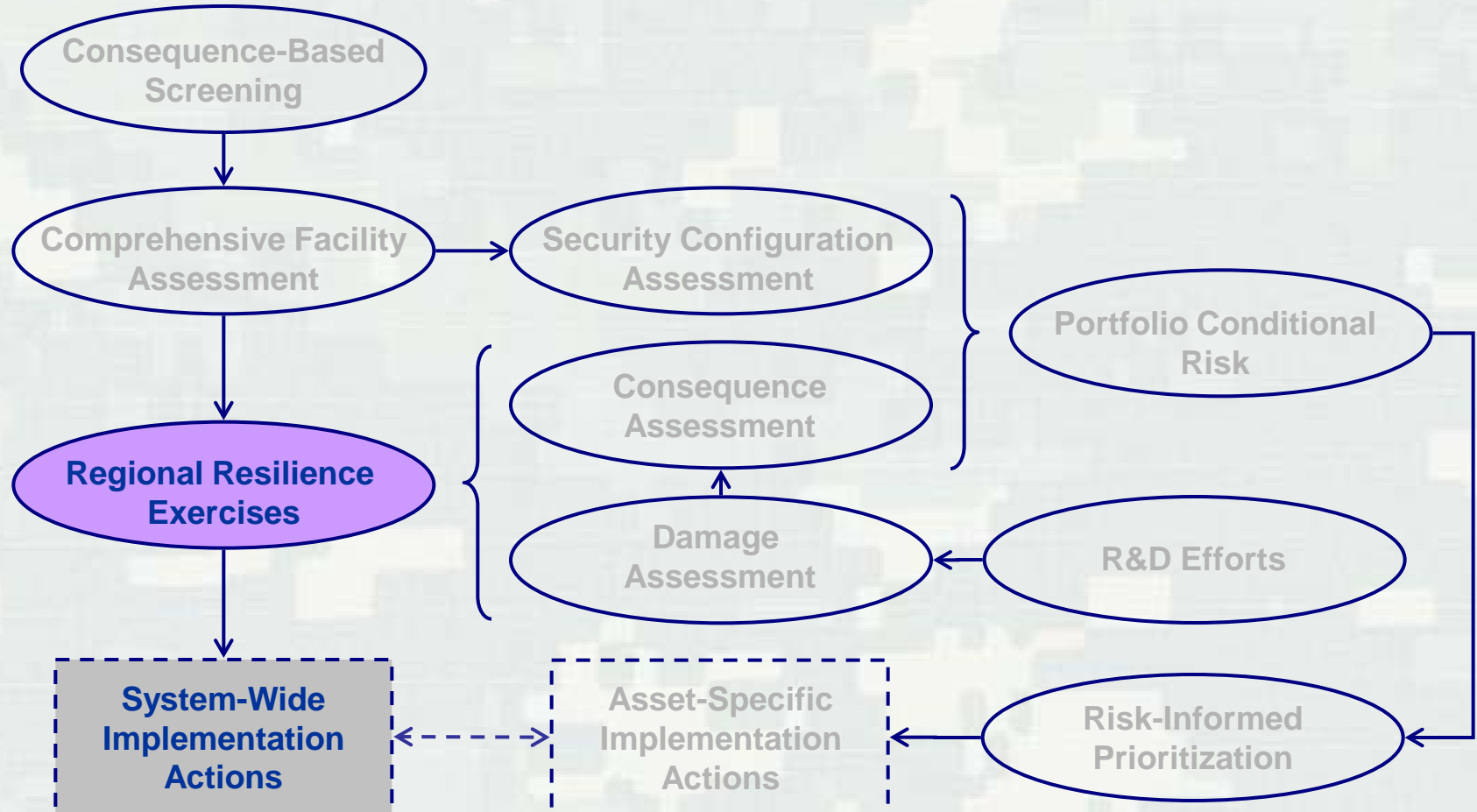


Integrated Approach for Enhanced Protection & Resilience



BUILDING STRONG®

USACE Critical Infrastructure Protection & Resilience (CIPR) Program



Regional Resilience Efforts: Dams Sector Exercise Series (DSES)

- Collaborative process to identify, analyze, assess, and enhance regional preparedness and disaster resilience involving a wide array of public & private stakeholders.
- For a given region, a particular scenario serves as the triggering event to analyze impacts, disruptions, critical infrastructure interdependencies, and stakeholder roles and responsibilities.
- Three major regional efforts conducted to date:
 - Bagnell/Truman Dams (DSES-08)
 - Columbia River Basin (DSES-09)
 - Green River Valley (DSES-10)



2010 Dams Sector Exercise Series – Green River Valley (DSES-10)

▪ Goals:

- Understand potential impacts associated with significant flooding events along the Green River Valley (State of Washington).
- Identify and prioritize critical infrastructure dependencies and interdependencies.
- Assist public/private stakeholders in improving recovery strategies and business continuity plans.



DSES-10 Approach

- Implemented through a series of discussion-based activities (meetings, seminars, workshops, etc), complemented by data gathering and analysis efforts.
- A systematic process is followed to consolidate findings, and support a framework to inform future resource requirements and investment justifications.
- Comprised of 3 major areas:
 - 1) Regional Baseline Assessment
 - 2) Regional Consequence Assessment
 - 3) Regional Resilience Strategy



DSES-10 Initial Planning Workshop

- Conducted on April 28, 2010 in Seattle, WA.
- Served as an effective forum to discuss the multiple aspects of the DSES-10 effort.
- Over 151 participants, including 114 Federal, State, and local government representatives, 27 private stakeholders, and 10 representatives from non-profit organizations.

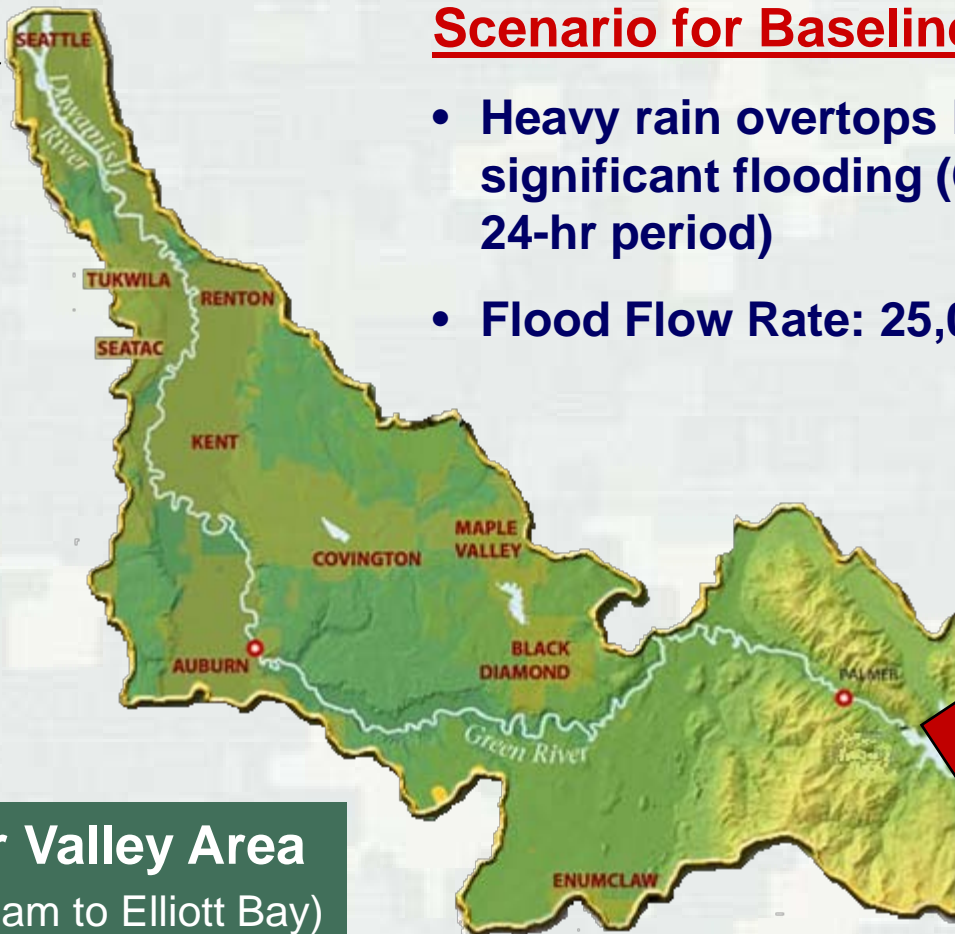


DSES-10 Triggering Event:
A significant flooding scenario affecting the King County communities of Auburn, Kent, Renton, and Tukwila.



Scenario and Geographic Scope

Harbor
Island
Area



Green River Valley Area
(62 miles from Dam to Elliott Bay)

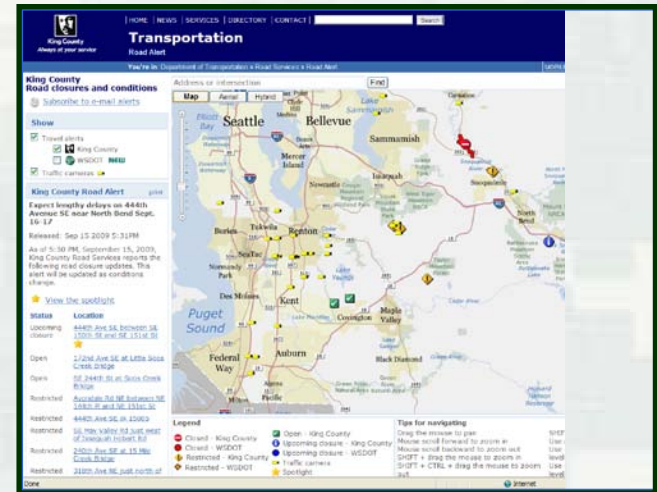
Scenario for Baseline Assessment:

- Heavy rain overtops levees resulting in significant flooding (6-in rain over a 24-hr period)
- Flood Flow Rate: 25,000 cfs

Howard
Hanson
Dam

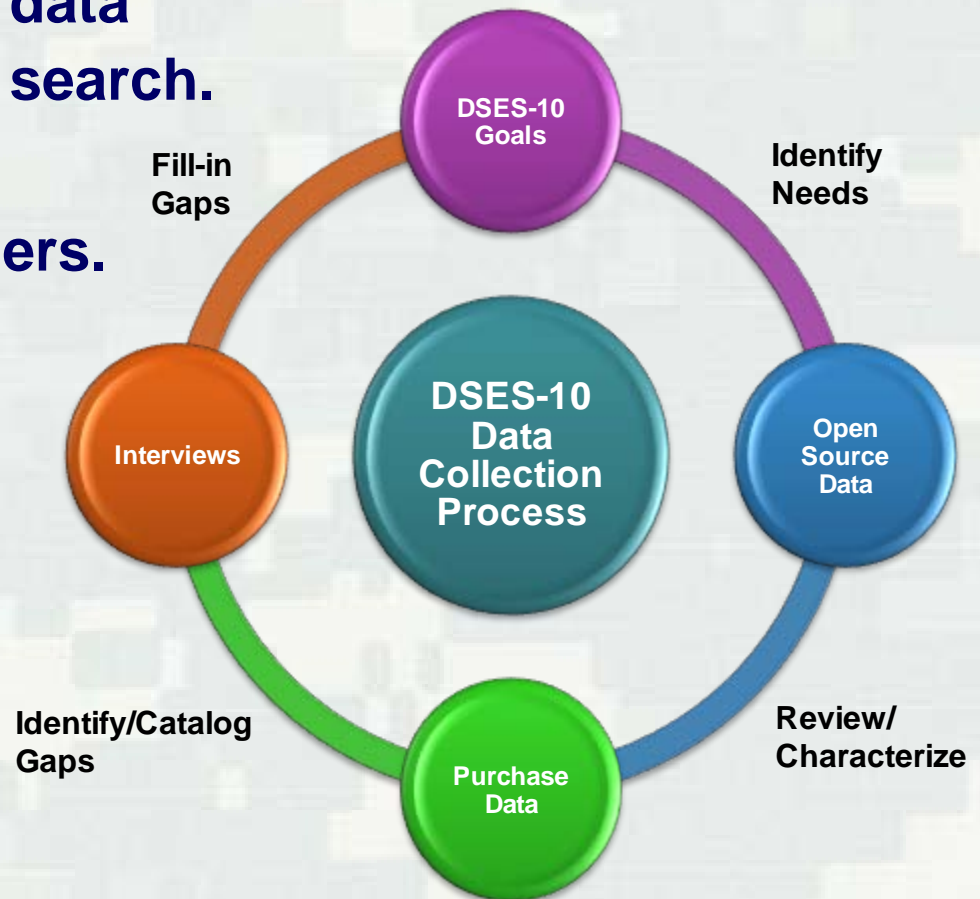
1) Regional Baseline Assessment

- Consolidate regional baseline information.
 - Economic structure, industrial development, social landscape.
 - Potential disruption scenarios.
- Identify current public and private capabilities.
 - Preparedness, mitigation, response, and recovery.
- Identify information sharing and collaboration mechanisms used during disaster lifecycle.
- Assess infrastructure interdependencies.



Data Collection Process

- Leverage from previous studies and regional workshops.
- Conduct “open source” data collection and literature search.
- Interview process with public/private stakeholders.
 - State and local
 - Private owners
 - Non-profit organizations

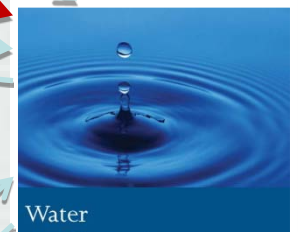
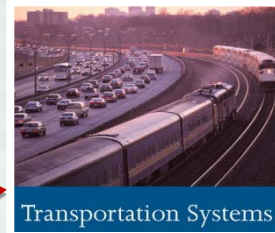


Cross-Sector Interdependencies



Flooding Scenario

- Airports
- Roads
- Railroads



A disruption in one critical infrastructure sector may impact other(s) critical infrastructure sector(s).

- Natural gas pipelines
- Oil terminals; Pump stations
- Electric substations

- Water facilities
- Wastewater facilities

18 Critical Infrastructure Sectors

Sector Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture* Department of Health and Human Services*	Agriculture and Food
Department of Defense*	Defense Industrial Base
Department of Energy	Energy*
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water*
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration United States Coast Guard	Transportation Systems*
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities*

DSES-10 Regional Baseline Assessment Workshop

- Conducted on June 30, 2010 in Seattle, WA.
- Served as a working session to review and evaluate ongoing regional baseline assessment, discuss preliminary findings, and gather active feedback and recommendations from regional stakeholders.
- Over 65 participants from Green River Valley public and private stakeholders.

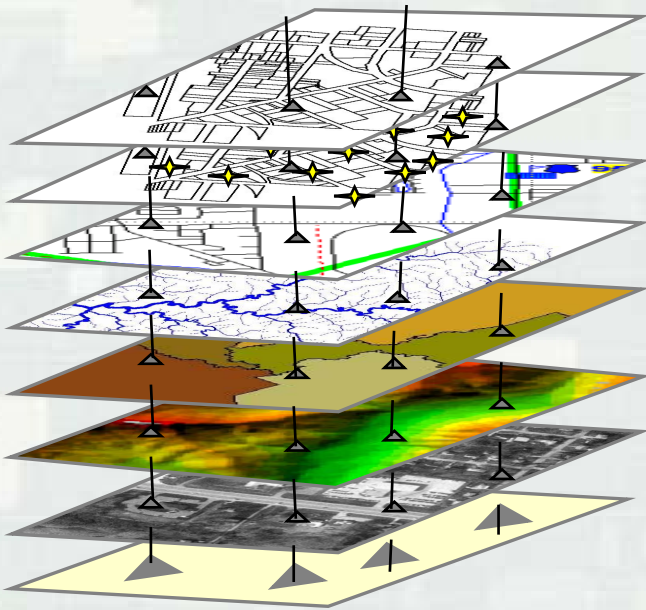


2) Regional Consequence Assessment

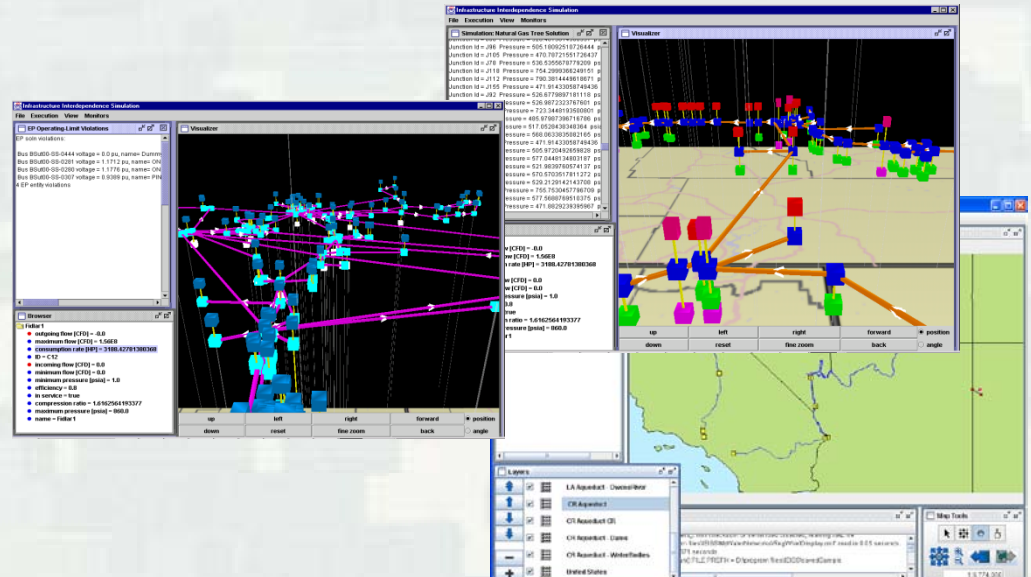
- Estimate extent of regional direct and indirect consequences associated with significant flood events.
- Refine existing models and procedures to assess regional short-term and long-term impacts associated with significant disruption scenarios.
- Conduct scenario-specific identification of critical infrastructure dependencies and interdependencies.



Critical Infrastructure Interdependencies

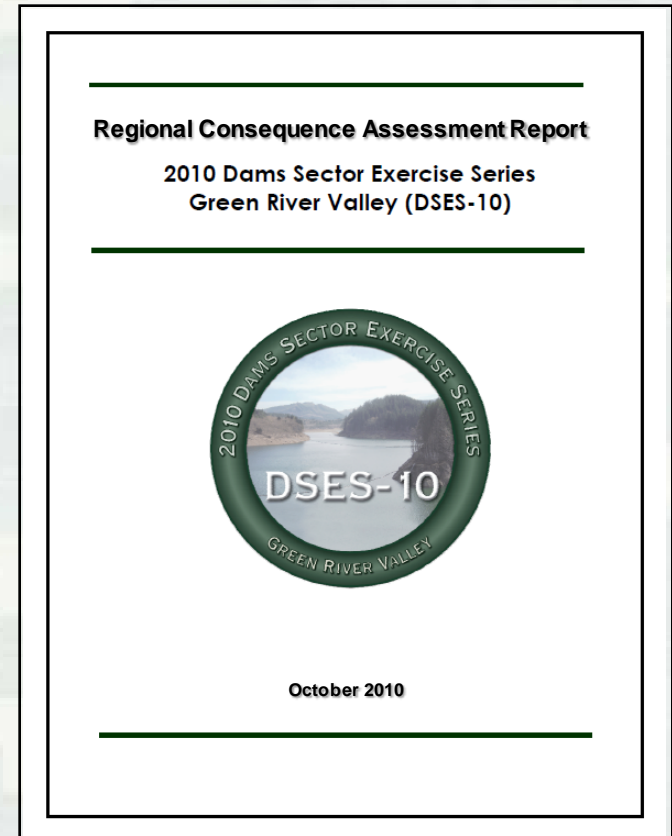


- **Electric Power**
- **Natural Gas/Crude Oil**
- **Telecommunications**
- **Water**
- **Healthcare/Public Health**



DSES-10 Regional Consequence Assessment Workshop

- **Scheduled for October 21, 2010 in Seattle, WA.**
- **Working session to review and discuss regional consequence assessment preliminary findings, and gather feedback and recommendations from regional stakeholders.**
- **Participants will include Green River Valley public and private stakeholders.**



3) Regional Resilience Strategy

- Assist public and private stakeholders in jointly enhancing regional resilience.
- Support identification of integrated post-disaster recovery solutions and prioritize recommended short-term and long-term actions to improve regional disaster resilience.
- Identify regional strategy implementation mechanisms and support strategic flood risk reduction efforts and other interagency initiatives.



Towards and Integrated Outcome

DSES-10

**Regional
Baseline
Assessment**

**Regional
Consequence
Assessment**

**Regional
Resilience
Strategy**



BUILDING STRONG®



**US Army Corps
of Engineers ®**

For Additional Information:

**Yazmin Seda-Sanabria
Senior Program Manager, CIPR
U.S. Army Corps of Engineers, Headquarters
Office of Homeland Security
Washington, DC
Email: Yazmin.Seda-Sanabria@usace.army.mil**




**International Federation
of Red Cross and Red Crescent Societies**

[français](#)
[español](#)

Search :

[Home](#)
[How to help](#)
[Who we are](#)
[What we do](#)
[Where we work](#)
[News](#)
[Meetings & events](#)
[Photo galleries](#)
[Publications](#)
[Directory](#)
[Jobs](#)
[Volunteers](#)
[Youth](#)
[Contact us](#)
[Search](#)

One year on – Strong signs of recovery follow September 2009 disasters in Asia-Pacific

In September 2009 four countries in the Asia-Pacific region – the Philippines, Indonesia, Vietnam and Samoa – were reeling from the impact of consecutive natural disasters that struck over a one-week period. More than 2,500 people perished and almost 11 million people were directly affected when the region suffered the combined impact of typhoons, an earthquake and a tsunami. Today, those same communities have made dramatic steps towards recovery, infrastructure has been repaired, water supplies restored and people who lost their homes once more have a roof over their heads.



- ▶ [Read the press release](#)
- ▶ [Read the news story: Philippines - one year after typhoon Ketsana](#)
- ▶ Follow us on [Facebook](#), [Twitter](#) and [YouTube](#)
- ▶ [Latest Red Cross Red Crescent news](#)



Haiti: Port-au-Prince lashed by violent storm

Almost 2,300 families are left in need of new shelter after a storm hit Haiti on Friday.



Pakistan: concerns over food security

IFRC and Pakistan Red Crescent start planning for the longer term recovery.

TOP ISSUES



World Disasters Report 2010

IFRC warns that 2.57 billion urban dwellers living in low and middle income nations are exposed to unacceptable levels of risk.



MDG Summit

IFRC and its partners has convened two side events at the MDG Summit with a focus on immunization and malaria.



Influenza pandemic

Preparation and response in

GET INVOLVED


[Donate online | Bank transfer](#)


[Become a volunteer](#)


[Youth activities](#)


[Contact your National Society](#)

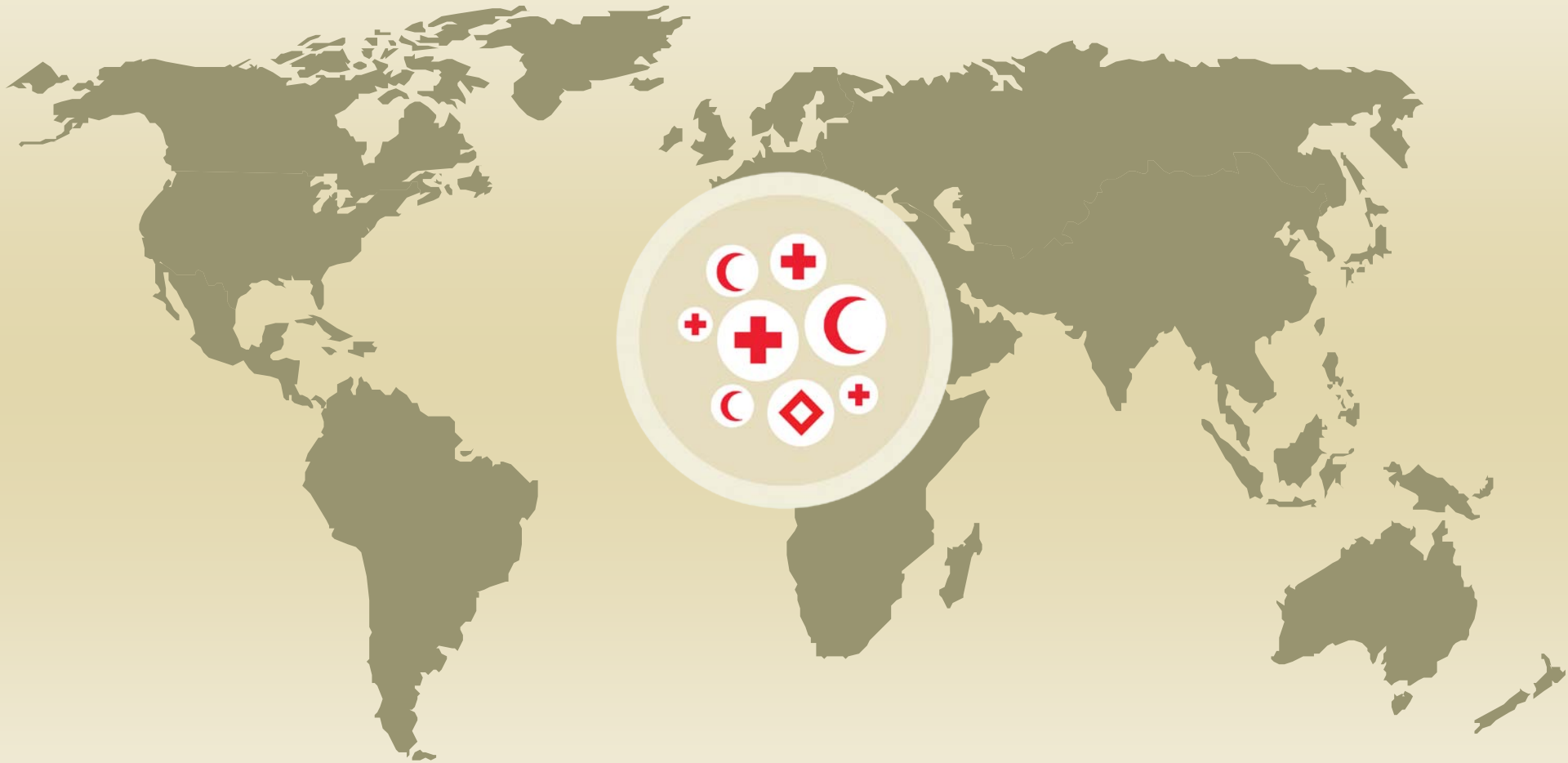
[SHARE](#)

PHOTO GALLERIES

International Federation of Red Cross and Red Crescent Societies

International Federation of Red Cross and Red Crescent Societies

- The Federation carries out *relief operations to assist victims of disasters*, and combines this with development work to strengthen the capacities of its member National Societies.
- The Federation's work focuses on *four core areas: promoting humanitarian values, disaster response, disaster preparedness, and health and community care*.
- 186 countries have Red Cross/Red Crescent societies.



More than 180 countries and 100 million volunteers

International Federation of Red Cross and Red Crescent Societies

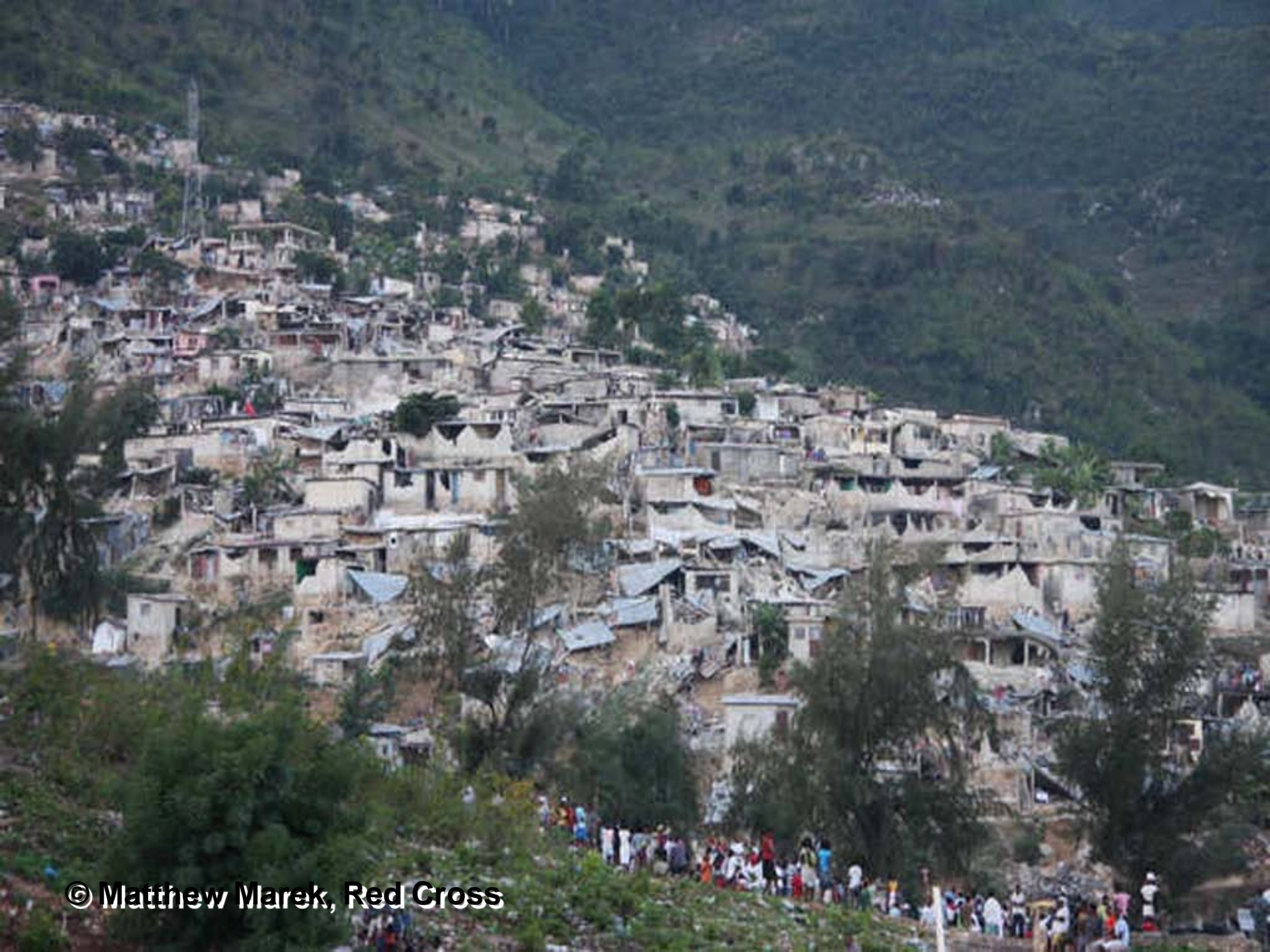
Each country is resourced differently, according to their unique skill sets:

- *Mexicans and Icelandic* perform Urban SAR
- *British* provide water sanitation
- *Germans and Norwegians* establish field hospitals
- *Americans* coordinate logistics, movement of materials

We provide *hope and help* around the world.



Earthquake in China



© Matthew Marek, Red Cross



© Matthew Marek, Red Cross



© Matthew Marek, Red Cross

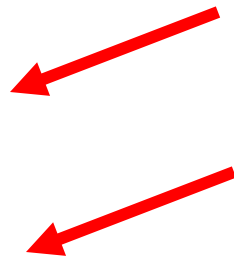
Phases of a Disaster

- **Rescue**
- **Response**
- **Recovery**
- **Rebuilding**

Phases of a Disaster

- **Rescue**
- **Response**
- **Recovery**
- **Rebuilding**

**The current
challenges in Haiti**







**The American Red Cross story
began on a battlefield.**



Clara Barton

The *modern* Red Cross


We **shelter, feed and care** for disaster victims.

We **supply** nearly half the nation's blood.

We **teach** lifesaving skills.

We **help** the military and their families.

We **provide** humanitarian aid worldwide.

A woman with long brown hair, wearing a pink top and a brown jacket, is smiling and looking towards the camera. She is standing in front of a large, vibrant mural. The mural features a bright yellow sun or moon in the upper center, with several blue birds flying around it. The background of the mural is a mix of warm colors like orange, red, and yellow, with some darker areas on the right side. The overall mood is positive and inspiring.

**Empowering ordinary
people to perform
extraordinary acts.**

**Preparation is critical to fast,
effective disaster response.**





Each year we train
10 million people.



**We serve members of the military, veterans
and their families.**





**Every two seconds, someone
needs blood.**



**We respond to
70,000 disasters a
year.**





Midwest Floods



American
Red Cross

ASTER
ICES

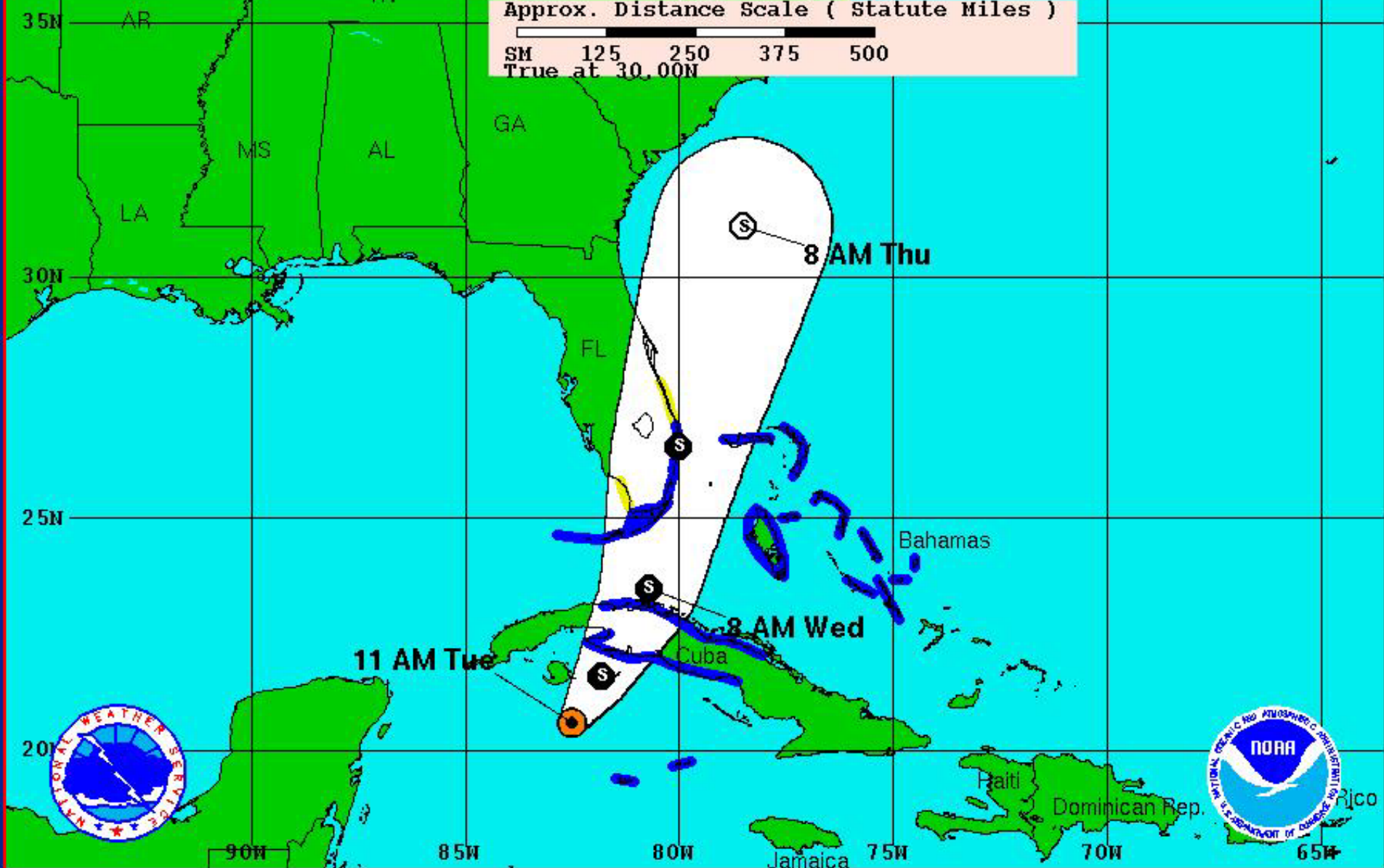
All American Red Cross
Disaster Assistance Is Free





“Tropical Depression 16”

Rainfall: The depression is expected to produce 5 to 10 inches of rain over the Cayman Islands, Jamaica, and Cuba. Isolated maximum amounts of 20 inches are possible over the higher elevations of Cuba and Jamaica. These rains could cause life-threatening flash floods and mud slides.



Tropical Depression Sixteen

Tuesday September 28, 2010

11 AM EDT Advisory 1

NWS TPC/National Hurricane Center

Current Information:

Center Location 20.6 N 82.5 W

Max Sustained Wind 35 mph

Movement NNE at 10 mph

Forecast Positions:

● Tropical Cyclone ○ Post-Tropical

Sustained Winds: D < 39 mph

S 39-73 mph H 74-110 mph M > 110mph

Potential Track Area:

Watches:

Warnings:

Disaster Services Mission Statement

The American Red Cross,
a humanitarian organization led by volunteers,
guided by its Congressional Charter and the
Fundamental Principles of the International Red Cross
Movement, will **provide relief to victims of**
disasters and help people prevent, prepare for, and
respond to emergencies.

Mission: *Disaster Services is America's partner and a leader in mobilizing communities to help people prevent, prepare for, respond to and recover from disasters and other life-threatening emergencies.*

Range of Responses

70,000 disasters a year, including:

- House fires and apartment fires
- Tornadoes, Floods, Winter storms, Hurricanes, and Earthquakes
- Transportation Incidents
- Terrorist events



When Disasters Occur

What We Do:

- Feeding, sheltering
- Distribution of emergency supplies
- One-on-one casework/assistance
- Health Services
- Mental Health
- Family Connectedness
- Community Recovery
- Blood & Blood Products



Current Capabilities: Feeding

- Maximum Meals Served in a Day

- 2004 – Charlie: 280,000
- 2005 – Katrina/Rita/Wilma: 995,000



- Today – Resources

- Ability to distribute > **1,000,000 meals/day**
- More than 300 Emergency Response Vehicles to deliver food and supplies, and 5 mobile kitchens
- With partners (Southern Baptists and others), provide significant capacity for meal preparation
- Stockpile of shelf-stable meals and shelter supplies has been integrated with DHS/FEMA stocks

Current Capabilities: Sheltering

- **Maximum Single Night Shelter Requirements**
 - Katrina: 140,000
- **Today – Resources**
 - 501,424 cots and 750,000 blankets
 - 327,104 comfort kits and 375,121 clean-up kits
 - National Shelter System (NSS) shows more than 50,000 potential shelters with the capacity to shelter millions
 - Sheltering limited by available facilities and trained staff



Partnerships



NATIONAL VOLUNTARY ORGANIZATIONS
ACTIVE IN DISASTER, INC.



The
National
Association of
Judiciary
Interpreters and
Translators



Boat People SOS

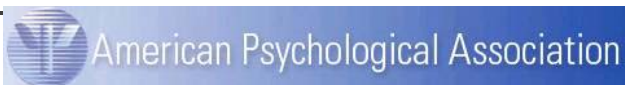
United Jewish
Communities
The Federation of Jewish Communities (New York City)



THE HUMANE SOCIETY
OF THE UNITED STATES



Tzu Chi Foundation



When Disasters are not Occurring - Readiness / Preparedness

- Capacity building and risk planning
- Pre-positioned supplies, shelters
- Volunteer recruitment & training
- Disaster plans & drills
- Planning & engaging key partners
- Community outreach & mobilization



Individual Preparedness

- Disasters or other emergencies can strike quickly and without warning
- The best way to make your family and you safer is to be prepared before disaster strikes:
 - Get a Kit
 - Make a Plan
 - Be Informed



Sample Preparedness Information

Be Red Cross Ready

Get a kit. Make a plan. Be informed.

It's important to prepare for possible disasters and other emergencies. Having a disaster kit, a plan, and information can help you and your family stay safe.

Prepárate con la Cruz Roja
Seguridad contra los terremotos

Los terremotos son un hecho natural que puede ocurrir en cualquier momento. Prepararse puede ayudarte a protegerte y a salvar vidas.

Be Red Cross Ready
Flood Safety Checklist

Know the Difference
Floods are among the most common natural disasters. They can be caused by heavy rain, melting snow, or a broken dam.

Prepárate con la Cruz Roja
Seguridad para las mascotas en caso de desastres

Las mascotas son parte importante de tu familia. Prepárate para protegerlas en caso de un desastre.

Be Red Cross Ready
Tornado Safety Checklist

Know the Difference
A tornado is a violently rotating column of air extending from a thunderstorm to the ground.

Be Red Cross Ready
Wild Fire Safety Checklist

Know the Difference
Wildfires are fires that burn out of control in wooded areas or on dry grass.

Prepárate con la Cruz Roja

El cuidado de personas con gripe

Si tienes a alguien en casa que tiene gripe, asegúrate de tener los suministros necesarios para cuidarlo.

Be Red Cross Ready
Swimming Safety in Lakes, Rivers and Streams

Swimming in lakes, rivers and streams can be fun, but it can also be dangerous. Follow these safety tips.

Be Red Cross Ready
Power Outage Checklist

Know the Difference
Power outages can happen at any time. Be prepared with backup power sources.

Be Red Cross Ready
Winter Storm Safety Checklist

Know the Difference
Winter storms can bring heavy snow, ice, and freezing temperatures.

Be Red Cross Ready
Thunderstorm Safety Checklist

Know the Difference
Thunderstorms can bring heavy rain, lightning, and hail.

Be Red Cross Ready

Hurricane Safety Checklist

Hurricanes are strong storms that cause life- and property-threatening hazards such as flooding, storm surge, high winds and tornadoes.

Preparation is the best protection against the dangers of a hurricane.

What should I do?

- Listen to a NOAA Weather Radio for critical information from the National Weather Service (NWS).
- Check your disaster supplies and replace or restock as needed.
- Bring in anything that can be picked up.

What supplies do I need?

- Water—at least a 3-day supply; one gallon per person per day
- Food—at least a 3-day supply of non-perishable, easy-to-prepare food
- Flashlight

What do I do after a hurricane?

- Continue listening to a NOAA Weather Radio or the local news for the latest updates.
- Stay alert for extended rainfall and subsequent flooding even after the hurricane or tropical storm has ended.

When a Watch Is Issued

- ▶ Listen for weather updates. Hurricanes are unpredictable, so stay informed.
- ▶ Have your car ready. Check gas, oil, water and maintenance.
- ▶ Check your disaster supplies kit.
- ▶ Close all windows and doors and then hurricane shutters. If you don't have shutters, close and board up all doors and windows with plywood. When windows break, homes are destroyed.
- ▶ Bring in bicycles, lawn furniture, hanging plants, trash cans or anything that could be picked up by strong winds.
- ▶ Secure your boat. Remember that most drawbridges and swing bridges will be closed to all boat traffic after the evacuation order is issued.



The American Red Cross

95% of our workforce are volunteers.

- **The American Red Cross has 33,000 paid staff and 700,000 volunteers.**
- **Most staff spend much of their time working with volunteers.**

Our Challenges?

Fundraising

The economy

Competing with other charities

Certain disasters (e.g. floods) are less compelling than others

Our Challenges?

Social Media

**How to harness the communication of the public and its
broad array of communication channels?**

Our Challenges?

Volunteer Engagement

**Like a volunteer fire department,
our volunteers can often go months
without a major call-out.**

95% of our workforce
are volunteers.

The American Red Cross has 33,000 paid staff and 700,000 volunteers.

Most staff spend much of their time working with volunteers.

In closing...

WHAT EXACTLY does the American Red Cross
do during a major disaster? ? ?

The American Red Cross establishes a relief operation equivalent to a Fortune 500 corporation

- fully staffed;
- internal and external voice and data communications;
- leadership teams utilizing timely data reporting;
- ... and we do it in 48 hours

The American Red Cross establishes a relief operation equivalent to a Fortune 500 corporation

- The facility we use may be an empty building a schoolhouse, or a former retail store;
- We have to turn it into an office space and run cables for connectivity;
- If communications are down, we bring our own, including satellite trucks.

The American Red Cross establishes a relief operation equivalent to a Fortune 500 corporation

- We will often bring together thousands of people with very specialized skills — the vast majority of them volunteers;
- We transport them, house them, and feed them;
- We see to their physical and emotional well-being;
- ...and in three weeks, we rotate that staff.

**The American Red Cross
establishes a relief operation
equivalent to a Fortune 500 corporation**

*And 91 cents on every donated dollar
goes to service delivery.*

Thank You

(Please wake the person next to you.)







Urban Search and Rescue

RESPONSE TO THE HAITI EARTHQUAKE DISASTER



Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Urban Search and Rescue

- Tech Rescue started in mid-1970s
- Two Federal Government agencies sponsor the team
 - USAID/OFDA (2 Teams)
 - DHS/FEMA (28 Teams)
- Specialize in rescue from reinforced concrete structures





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Team Expectations

- Report to POD within 6 hrs
- Air / ground mobile
- Self-sufficient for 72 hours
- Up to 10 day deployment
- 24 hour operation at 2 sites



Victim First



Response to the Haiti Earthquake Disaster

Full Team Deployments

– Armenia	Earthquake
– Philippines	Earthquake
– Oklahoma	Terrorist Attack
– North Carolina	Hurricane Fran
– Nairobi, Kenya	Terrorist Attack
– Izmit, Turkey	Earthquake
– Toulou, Taiwan	Earthquake
– Duzce, Turkey	Earthquake
– Virginia (Pentagon)	Terrorist Attack
– Bam, Iran	Earthquake
– Mississippi/Louisiana	Hurricane Katrina
– Virginia	Hurricane Ophelia
– Texas	Hurricane Rita
– Florida	Hurricane Ernesto
– Georgia	Hurricane Gustav
– Louisiana	Hurricane Ike
– Pétionville, Haiti	Structure Collapse
– Port-au-Prince, Haiti	Earthquake



Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Task Force Components:

— Search





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Task Force Components:

- Search
- Rescue





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Task Force Components:

- Search
- Rescue
- Medical





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Task Force Components:

- Search
- Rescue
- Medical
- Command and General Staff





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Task Force Components:

- Search
- Rescue
- Medical
- Command and General Staff
- Logistics





Response to the Haiti Earthquake Disaster

Earthquake Details

- 7.0 magnitude Earthquake strikes January 12, 2010, at 1653 hours
- Epicenter about 10 miles southwest of Port-au-Prince, Haiti
- Most powerful earthquake to hit Haiti in a century
- Initial media reports suggested:
 - High number of casualties (100K-200K)
 - Widespread damage
 - Urgent need for Search and Rescue

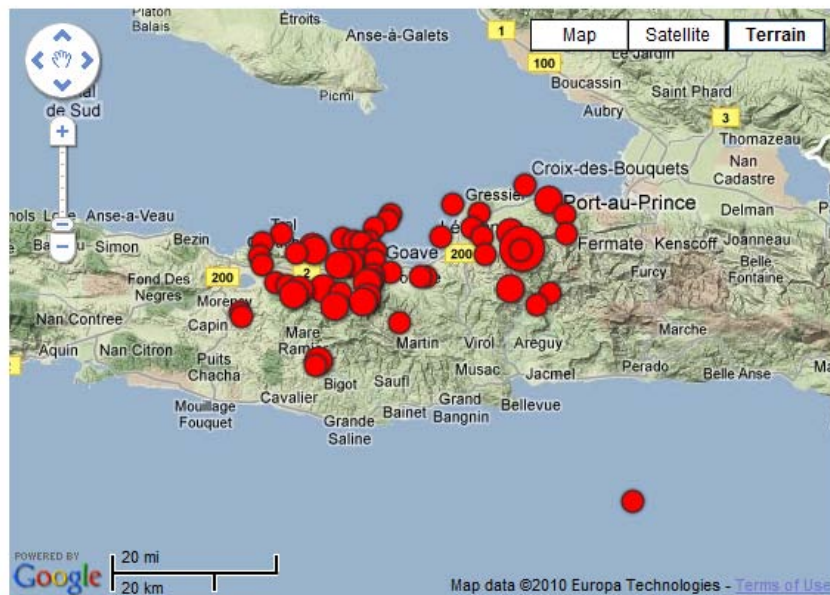




Response to the Haiti Earthquake Disaster

Earthquake Details

- Aftershocks from 1/12/2010 – 2/5/2010
 - M6.0 occurred 7 minutes after quake
 - M5.9 occurred 1/20/2010
 - 16 at M5.0 or greater
 - 59 at M4.5 or greater





Response to the Haiti Earthquake Disaster

Port-au-Prince, Haiti Details

- Area: 14.7 square miles
- Population: 1,000,000+
- Density: 70,000 / square mile
- Experience: 2008 School Collapse



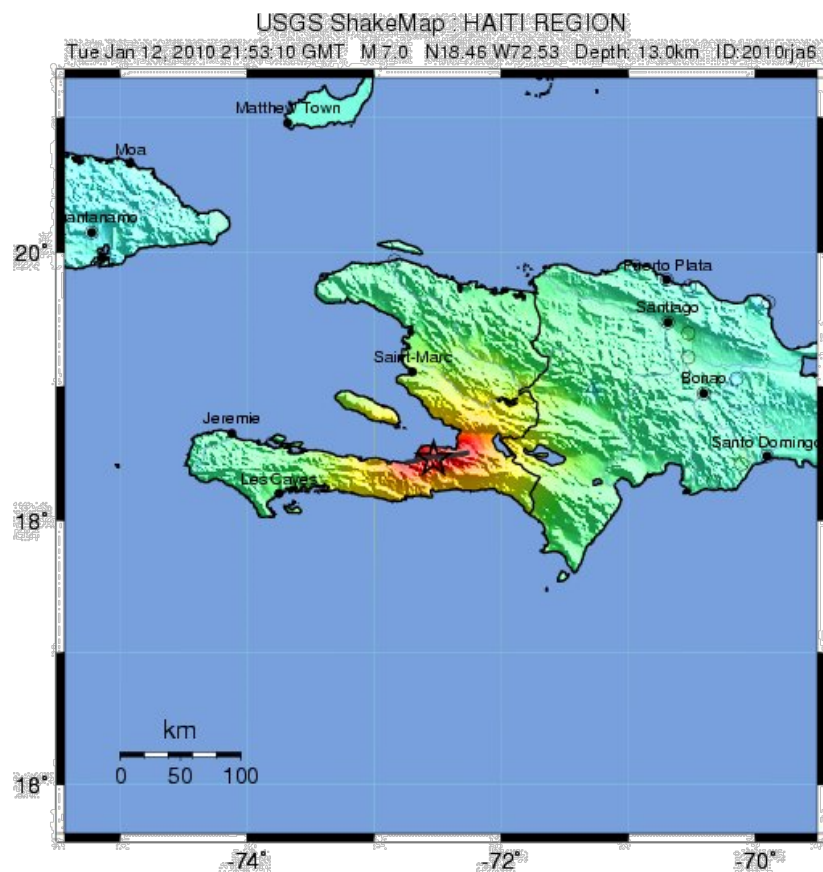


Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Activation

- 38 minutes later USAID mobilizes:
 - USA1
 - USA2
 - AST
 - UNDAC Member
- Fastest deployment decision to date from USAID
- Mobilization process begins



12 January 2010

Victim First



Urban Search and Rescue

Response to the Haiti Earthquake Disaster

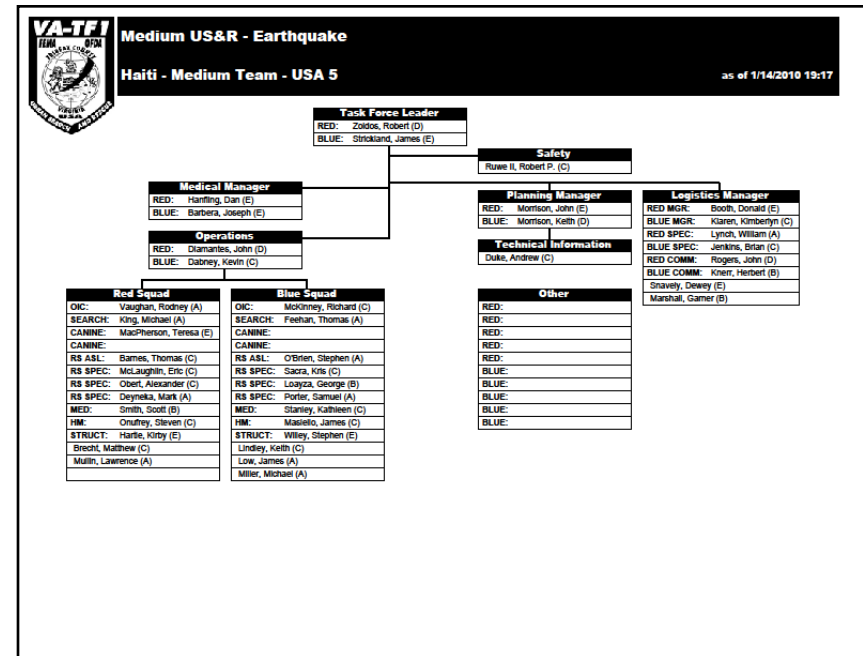
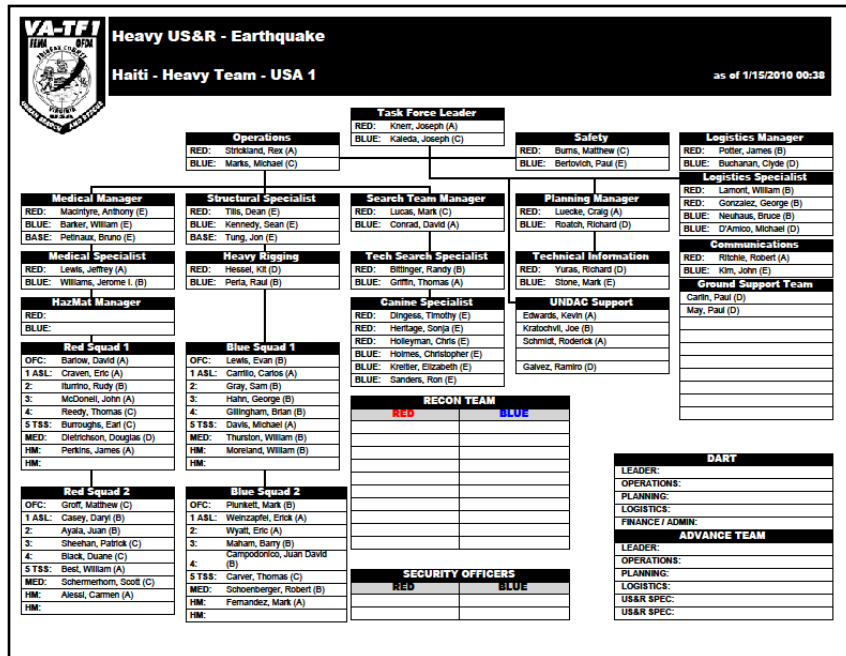
Team Configurations

USA-1 (Heavy)

- 72 members + 6 canines
- Arrived within 24 hours

USA-1 (Medium)

- 42 members + 1 canine
- Arrived within 60 hours



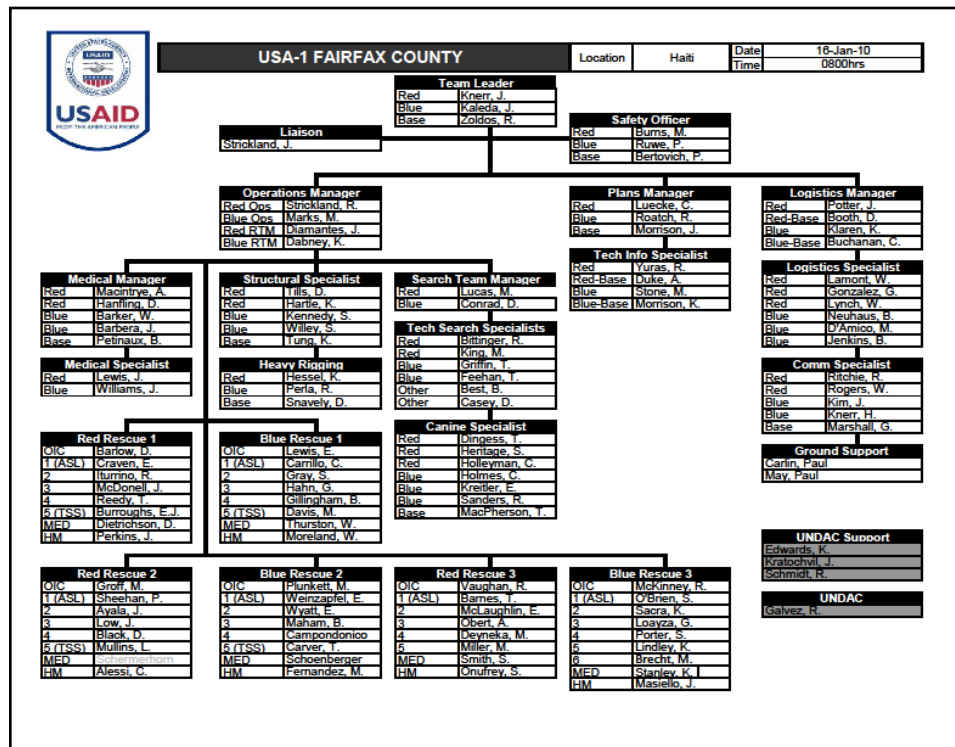


Response to the Haiti Earthquake Disaster

Team Configurations

USA-1 (Super Jumbo)

- Combined upon arrival of Medium Team
- 114 members + 7 canines





Response to the Haiti Earthquake Disaster

Operations

- Arrive at US Embassy around 2000 hrs
- BoO is being set up
 - BoO Site determined by the DART & RSO
 - Still an active embassy – evacuating American citizens
 - Benefit of Embassy vs. OSOCC:
 - Transportation
 - Water
 - Electricity
 - Security

2100 TFL's meeting with DART & ASO

- Priority building being assigned
- Security briefing
- Compound rules





Response to the Haiti Earthquake Disaster

Timeline of Operational Highlights

- 2245 UN Minustah Rescue of 1-37YOM
(Concluded 1-14-10 0742)



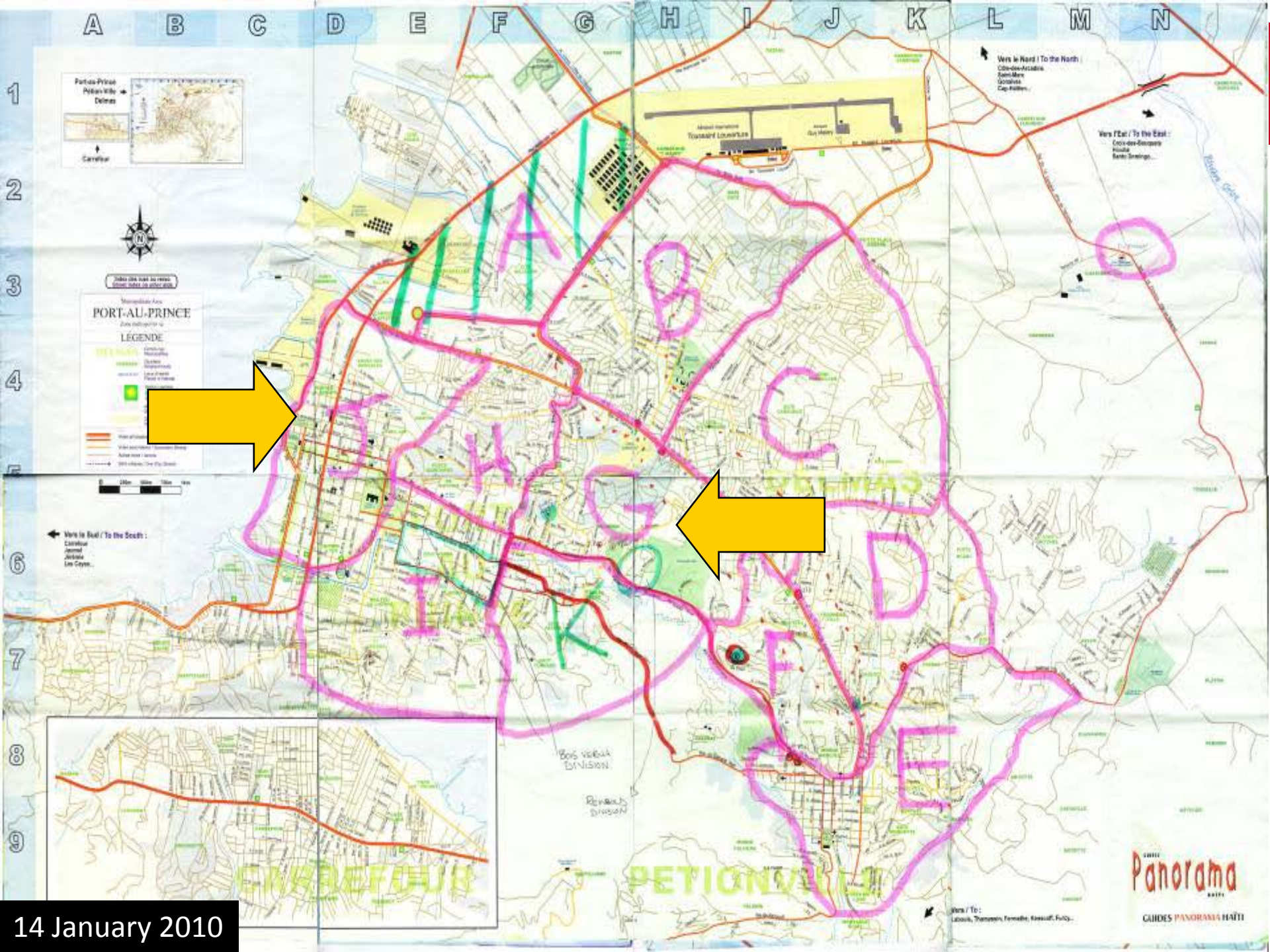


Response to the Haiti Earthquake Disaster

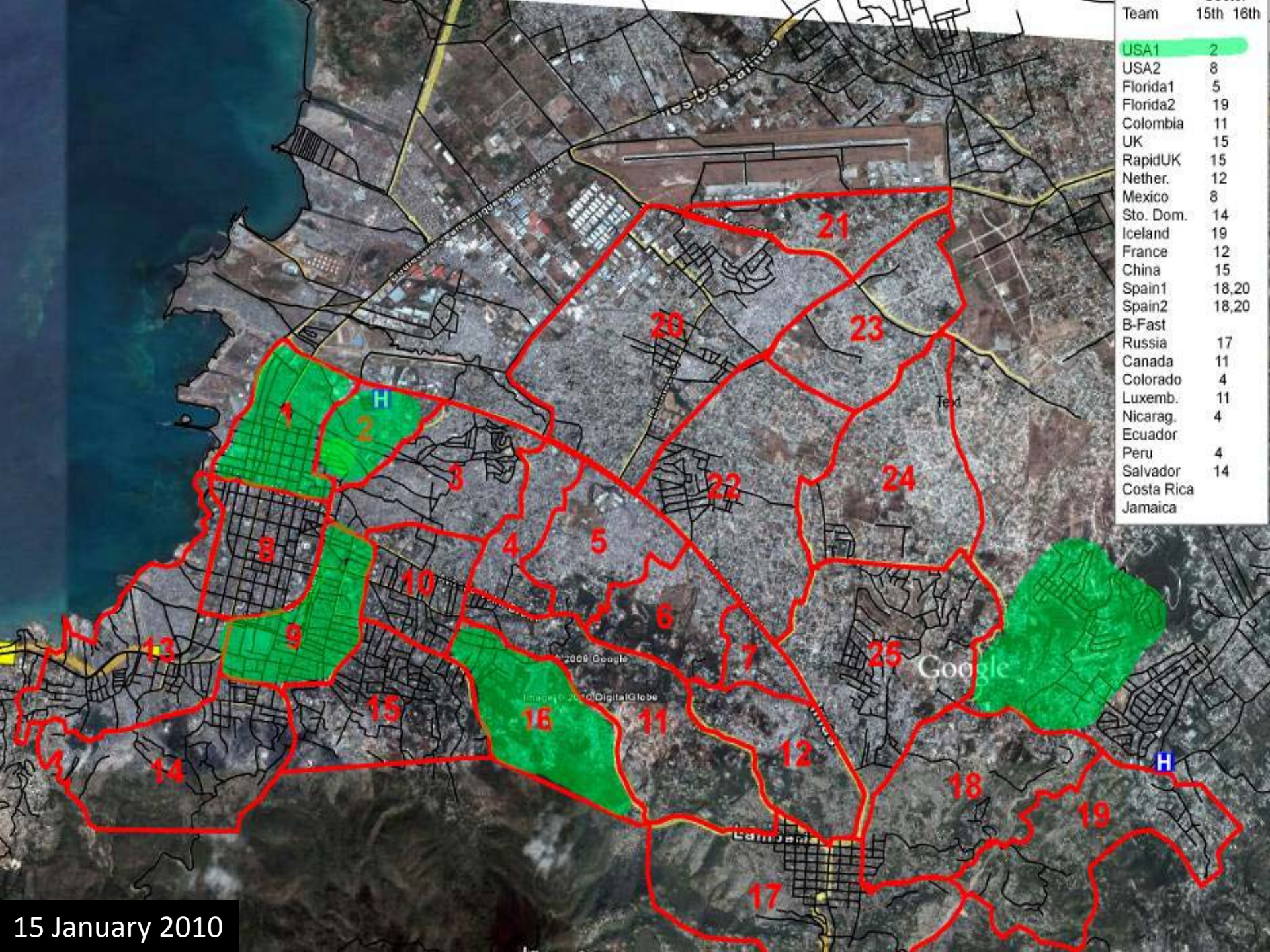
Timeline of Operational Highlights

- 0645 Hotel Montana Operations begin
- Numerous assignments from USAID-field assessments
- Rescue Squads and RECON squads in full "Blitz Mode"
- Coordinating operations with LAFD (USA2)
 - Develop and assign Divisions for PAP
- 1640 Recon assigned JULIET Division
 - 1830 diverted to assist Iceland at Caribbean Market
- 1705 Recon assigned GOLF Division
- Midnight - Units completed operations other than Hotel Montana
 - **16-Sites were searched**
 - **2-Divisions were searched**
 - **9-rescues were initiated**





14 January 2010



Team	15th	16th
USA1	2	
USA2	8	
Florida1	5	
Florida2	19	
Colombia	11	
UK	15	
RapidUK	15	
Nether.	12	
Mexico	8	
Sto. Dom.	14	
Iceland	19	
France	12	
China	15	
Spain1	18,20	
Spain2	18,20	
B-Fast		
Russia	17	
Canada	11	
Colorado	4	
Luxemb.	11	
Nicarag.	4	
Ecuador		
Peru	4	
Salvador	14	
Costa Rica		
Jamaica		

15 January 2010



Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Timeline of Operational Highlights

- GRID Search Sector-1 & 9
- 0915 Secondary Search of Hotel Christopher
- 1625 Olympic Market Rescue Assist (DAY 7)
- 911's



18 - 19 January 2010

Victim First



Urban Search and Rescue

Response to the Haiti Earthquake Disaster

Timeline of Operational Highlights

- 6.1 Magnitude Earthquake
- GRID Search EQ Epicenter
- Carrefour Search Investigations
- 911's
- Begin Humanitarian Aid
 - St François Pediatric Hospital Tent Project
 - De L' Ofatma Hospital Shoring Project
 - Hotel Napoli Investigation
 - Equipment Donations



20 - 23 January 2010



Response to the Haiti Earthquake Disaster

Operations-The Hotel Montana

- Extremely large resort style hotel.
- Five stories tall in most places.
- Team members made multiple rescues from site during the first few days.
- USA-1 established a continuous presence at the site on January 19 that would continue until relieved by the US Army Corps of Engineers on the January 25.
- Team started the systematic delayering of the structure and established command of the area to include body identification and forensic efforts.





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

The Hotel Monana [Structural Stability]

- Multiple Stories in pancake and other style collapses
- Simultaneous multi-team operations





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

The Hotel Montana [Multiple Worksites]

- Command and control difficult at such a large site.
- Up to eight different teams working simultaneously speaking several languages.





Urban Search and Rescue

Response to the Haiti Earthquake Disaster

The Hotel Montana [Political Concerns]

- Multi-government interest in the site.
- Press onsite at all times.
- Several congressional “tours”





Response to the Haiti Earthquake Disaster

Accountability and Documentation

- All Rescue Teams
 - 67 teams
 - 1,918 staff and 160 dogs
 - 130+ rescues
- VA-TF1
 - 114 staff and 7 dogs
 - 16 rescues
 - 9 unassisted
 - 7 assisted





Sharing Intelligence and Managing Risk Across the Homeland Security Enterprise

NDIA Symposium 2010

Caryn Wagner

Under Secretary for Intelligence and Analysis

Chief Intelligence Officer

U.S. Department of Homeland Security

September 28, 2010



Homeland
Security

The Homeland Security Space is Complex



9/11 Terrorist Attacks



Cyber Attacks



Hurricane Katrina
Flooding



Tropical Storms

Intelligence and risk information are key to operating in this complex mission space



**Homeland
Security**

Threats and Global Challenges

From the 2010 Quadrennial Homeland Security Review

Major Threats	Global Challenges
High-Consequence Weapons of Mass Destruction	Economic and Financial Instability
Al-Qaeda and Global Violent Extremism	Dependence on Fossil Fuels and the Threats of Global Climate Change
Illicit Trafficking and Related Transnational Crime	Nations Unwilling To Abide by International Norms
Pandemics, Major Accidents, and Natural Hazards	Sophisticated and Broadly Available Technology
High-Consequence and/or Wide-Scale Cyber Attacks, Intrusions, Disruptions, and Exploitations	Other Drivers of Illicit, Dangerous, or Uncontrolled Movement of People and Goods
Smaller Scale Terrorism	

“Ultimately, homeland security is about effectively managing risks to the Nation’s security”



**Homeland
Security**

What is Risk?



Can be viewed as a function of:

- Threat
- Vulnerability
- Consequences

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

DHS Risk Lexicon, 2nd Edition, 2010



**Homeland
Security**

What is Risk Management?

Risk management is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken

DHS Risk Lexicon, 2nd Edition, 2010



DHS Interim Integrated Risk Management Framework, 2009



**Homeland
Security**

Intelligence is Key to the Risk Management Cycle



DHS Risk Management Process



Intelligence Cycle



**Homeland
Security**

The Value of Integrated Risk Management

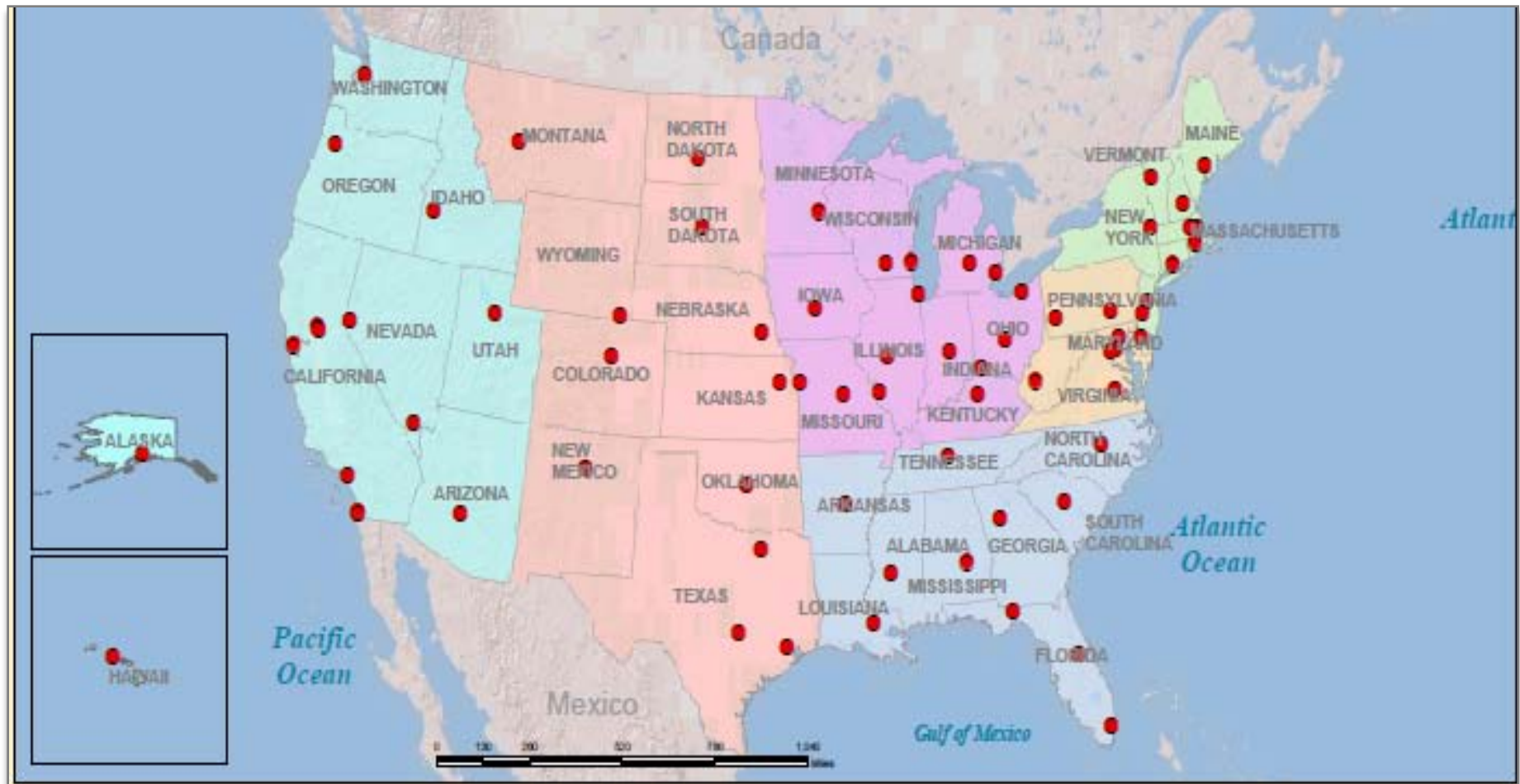
- Allows for more transparent and defensible decision making
- Contextualizes homeland security threats, showing which are the most likely and highest impact
- Informs prioritization decisions between terrorism, natural disasters, cyber, pandemics, border security and transnational crime
- Provides a performance measure for programs across the homeland security mission space
- Identifies opportunities for reducing or transferring risk

Secretary Napolitano signed a Policy on Integrated Risk Management for the Department in May 2010



**Homeland
Security**

Sharing Risk and Intelligence Information with Partners



72 State and Major Urban Area Fusion Centers



**Homeland
Security**



Homeland Security



STRATIS

Powered by Excellence

2010 Homeland Security Symposium

Cyber Threats and Enhancing Security of the IT Infrastructure

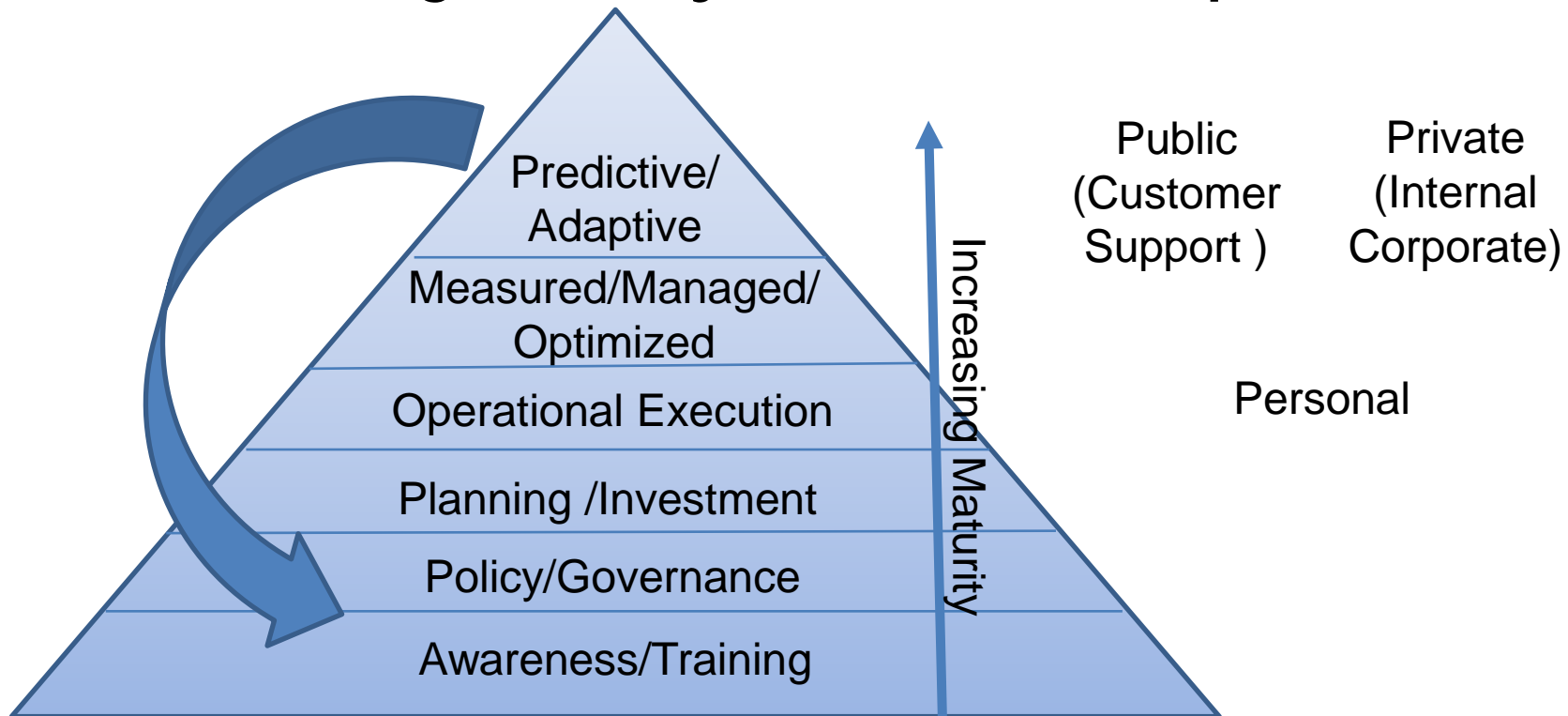
"This document consists of L-3 Services Inc. general information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) or Export Administration Regulations (EAR). Cleared by STRATIS Export Compliance (01/10)"



STRATIS
Powered by Excellence

Use of Standards in Security Maturation

- Increasing Maturity and Partnership



How do standards help US protection or facilitate attackers?



STRATIS
Powered by Excellence

Distributed Computing / Communications

- **Securing of .mil and .gov**
 - Gen. Alexander remarks for critical infrastructure as a separate network (.cif)
- **Distributed SCADA / critical infrastructure**
 - NIST Guidelines for Smart Grid Cyber Security
 - DHS training and standards for critical infrastructure protection (CIP)
- **Increasing mobile devices / telework trend**
 - e.g. Mobile banking and financial applications
 - Cloud consolidation facilitating mobility

Do we need voluntary and / or regulated standards for .cif ?